SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
CRIMTRAC

Question No. 135

Senator Ludwig asked the following question at the hearing on 31 October 2005:

The handheld devices:
(a) What sort of biometric data is stored?
(b) How is the information going to be secured?
(c) How is it going to be exchanged?
(d) How is it going to be kept on databases?
(e) When in the field, how are the devices going to be secured to ensure there is no accidental disclosure of information?
(f) Does the information include names?
(g) What is the cost of handheld devices?
(h) Have these issues been investigated and has it been determined that the devices are practical and safe and provide secure information that cannot be accidentally downloaded or passed on to other people outside of the required use or policing service?

The answer to the honourable senator's question is as follows:

(a) This will vary between vendor products. In general the devices can store both biometric "minutiae" maps linked to the associated demographic data or the maps can be linked to a reference number from a police agency information system (i.e. no demographic data or fingerprint images stored on the device). The data requirements have yet to be determined by the individual police services.

(b) This has not yet been determined but will be based upon State, Territory and Commonwealth data security requirements.

(c) The appropriate method of data transfer providing appropriate levels of data encryption and security has yet to be identified as part of a request for tender to purchase the technology (developed by jurisdictions and CrimTrac representatives in line with State and Territory and Commonwealth data security requirements). In general communication between the device can be achieved using GSM, direct network connection or via connection to policing digital networks via a mobile data terminal.

(d) The biometric server will store a "minutiae" map that corresponds to records held within CrimTrac NAFIS.

(e) This will be based upon State, Territory and Commonwealth data security requirements and operational policing policies.

(f) No.

(g) The cost is unknown at this stage. This would be based upon the number of devices purchased from a particular vendor and the level of police service customisation of the generic software required to be completed by a vendor.

(h) The capability that is being implemented by CrimTrac is designed to enable the technical feasibility and business operational trials of the hand held device technology with various police services. Although the capability to integrate a remote hand held work biometric device (fingerprint biometrics only) will be available as part of this upgrade, the trial and implementation of the hand held biometric devices is yet to be determined. Many of the issues raised by the Senator will be determined as part of the trial process.