AusCheck Amendment Bill 2009 – CrimTrac Submission

Background

CrimTrac was established on 1 July 2000 under an Inter-Governmental Agreement (IGA) between the Commonwealth, States and Territories. The IGA provides for the operation and governance of CrimTrac.

CrimTrac's primary role is to provide national information sharing solutions to support the effective operation of police services and law enforcement agencies across borders. The *CrimTrac Strategic Plan 2007-2010* requires CrimTrac to 'take a leadership role in generating national approaches to information sharing solutions for law enforcement agencies, for a safer Australia'. The agency's main functions include:

- Ensuring the secure, accurate and timely exchange of a broad range of information between law enforcement agencies in accordance with Australian law.
- Providing national criminal record checking services for law enforcement and other accredited agencies.
- Identifying, investigating and developing emerging information technologies, opportunities and information sharing solutions that would provide benefits to law enforcement agencies. The CrimTrac Strategic Plan outlines a number of such potential opportunities.
- Developing information sharing solutions that leverage of CrimTrac's core capabilities (for example utilising the national fingerprint system as a platform to host other agencies biometric solutions).

CrimTrac holds and brokers factually-based information. The collective information holdings of CrimTrac are significant and include:

- Person information (persons who have a warning; warrant; are wanted; offence history; criminal history; firearm; order; on bail; or are an unidentified person/body, missing person or escapee or are on the national child offender register)
- Vehicle information (vehicle, registration and driver licence information; stolen vehicle information)
- Firearm information (licence holders; adverse firearms licence history; licensed firearms dealers; lost, stolen and wanted firearm information)
- DNA profiles (de-identified)
- Fingerprints
- Photographs
- Child offender information (for registrable offenders).

As discussed CrimTrac undertakes national criminal record checking services. A National Criminal History Record Check (NCHRC) involves identifying and releasing any relevant criminal history information subject to relevant spent convictions/non-disclosure legislation and/or information release policies.

The information release policies include a requirement that any NCHRC must be done with the informed consent of the person being checked.

AusCheck is an accredited agency with CrimTrac for the purposes of NCHRC services and therefore results of a NCHRC are delivered to AusCheck directly and are utilised as part of AusCheck's background checking process.

Proposed amendments - Verification of Identity through the use of biometric data

CrimTrac is supportive of a proposal to use an individual's fingerprints or other biometric data to verify identity of individuals for national security background checking purposes.

In terms of CrimTrac's own name-based National Criminal Record Checking Service, CrimTrac holds some concerns about the use of name and proof of identity documentation as the sole means of confirming identity, particularly where criminal record checks are undertaken for pre-employment screening in high risk areas such as working with critical infrastructure and with vulnerable members of the community such as children and the aged.

It is noted that the wording in the explanatory memorandum gives the impression that AusCheck would only seek to collect and use biometric data where some inconsistency in the background checking process indicates that verification of identity is needed. Specifically the explanatory memorandum states that:

> "In conducting criminal history background checks it is sometimes necessary to confirm the identity of an individual so that police services can distinguish between people with the same or similar name and date of birth. In these circumstances, it may not be possible to complete the background check unless the identity of the individual can be confirmed through provision of further identification information such as fingerprints."

If it is not intended that identity verification documentation be routinely used as part of a national security background check, it should be noted by the committee that this may present a risk, for example, the name and date of birth provided by the applicant may appear legitimate however the applicant may have a criminal record under another identity in police systems that could only be linked through a biometric identifier.

Section 13(2) Collection, use and disclosure of identity verification information

Collection of biometric data

It is not obvious from the proposed amendments who would be responsible for collection of 'identity verification information' and whether that information would be searched against law enforcement holdings in order to verify identity. There is a reference in the explanatory memorandum which states that "if AusCheck is required to facilitate the provision of this information to the relevant police jurisdictions..."

CrimTrac is of the view that the value of verification of identity for background checking purposes through the use of biometric data is where a person's identity is checked against police biometric holdings to confirm whether that person is firstly in police systems, and secondly, if they are in police systems, that the identity is either the same as provided on their application or indicated that they have a different identity in police systems.

As you are likely aware, CrimTrac hosts the National Automated Fingerprint Identification System (NAFIS). This system stores fingerprints, palmprints and basic demographic information obtained from an individual by police services. The NAFIS accepts fingerprints taken by a range of methods, including the latest 'livescan' technology. This process enables police officers to enter the fingerprint records into NAFIS electronically for an immediate search against the national database, assisting police across Australia to establish identity from fingerprint and palm impressions quickly and reliably to resolve crimes.

The only way that AusCheck could check a person's identity using fingerprints against police holdings on a national basis is to utilise NAFIS. Australian police services collect fingerprints on local 'livescan' devices but do not hold fingerprint data on local systems. Whether AusCheck would arrange for fingerprints to be taken and submit as a physical copy to police as part of an application process to police or whether they would utilise police devices to collect fingerprints, the information would need to be loaded onto NAFIS even if it was for the purposes of one-off searching against the system rather than being stored on that system. The system would then match those tenprints against other tenprints held in the system (but not latent prints from crime scenes).

It would appear necessary for AusCheck to deliver effective identity verification services using fingerprints technology that fingerprints collected by AusCheck (or police services on their behalf) utilise the NAFIS as the mechanism for searching (and potentially storage if desired) of fingerprints.

Storage of biometric data

Section 13(2) does not refer to the storage of identity verification information. It is therefore presumed since the legislative amendment is silent on the issue that identity verification information is not intended to be stored on any database, including the AusCheck Database, even on a temporary basis. It is therefore understood that when a person reapplies for a card, licence, permit or other authorisation in relation to which a national security background check has been conducted, that they may have to resubmit biometric data.

In any event CrimTrac does not support the creation of a separate fingerprint repository for storage of biometric data if it is intended that data may at any stage be searched against police fingerprint holdings. This would raise issues of connectivity and quality standards and would involve the unnecessary duplication of effort and resources. CrimTrac is in the process of including fingerprints for other Commonwealth agencies within NAFIS. These agencies are Australian Fisheries Management Authority (AFMA) (illegal foreign fishers' fingerprints) and Department of Immigration and Citizenship (DIAC) (immigration detainees fingerprints). Fingerprints are able to be stored and managed in such as way as to meet agency requirements in terms of confidentiality, security and control of biometric information.

Use of biometric data

Section 13(2)(a) provides that the collection, use and disclosure of identity verification information about an individual is authorised by law if it is necessary for the purposes of verifying the identity of an individual in respect of whom a background check is being or has been conducted under the AusCheck Scheme.

National criminal record checks utilising a person's fingerprint are currently being undertaken using NAFIS in limited circumstances for persons seeking employment at casino and gaming venues; for persons working with dangerous goods; for employment with an Australian Police Service; to obtain handgun licences (in Victoria only) and in limited circumstances for persons applying for visas. These checks are not generally undertaken by CrimTrac, rather the police service for example would utilise NAFIS to verify a person's identity and then either conduct or arrange for an NCHRC to be conducted by CrimTrac on the verified name. AusCheck as an accredited agency with CrimTrac would be able to do the same following verification of identity of an individual through a fingerprint check by police and it is recommended that this occur as a matter of course, otherwise criminal record information on the verified identity would not be available for decision making purposes.

Disclosure of biometric data

It may be prudent in light of the above information for the proposed amendments to make explicit that 'identity verification information' could be disclosed to CrimTrac and Australian police services

for the purposes of verification of identity under s13(2). For example s15(2) of the *AusCheck Act 2007* allows for an authorised disclosure of personal information to be made to the Australian Federal Police for the purposes of the AusCheck Scheme.

Consent for background checks

Amendment 9 states that persons applying for an Aviation Security Identification Card (ASIC) or a Maritime Security Identification Card (MISC) or other card, licence, permit or authorisation are deemed to have given consent to a background check as part of their application. Amendment 9 futher states that applicants are to be advised that a background check is a precondition to the issuing of an ASIC, MISC or other card, licence, permit or authorisation.

This amendment seems to indicate that consent would be implied as a result of persons making applications for the above instruments. Consent obtained in this way may raise the issue of whether the person is fully aware of the extent of the background check to be undertaken and whether they have in fact consented to this. Any implied consent would therefore need to be sufficiently adequate to satisfy current Federal privacy provisions as they relate to background checks especially in relation to issues such as spent convictions. This may also raise concerns for privacy provisions in each of the States and Territories and should be considered to ensure that no conflict arises. Although applicants are to be advised of background checks as a precondition, the extent of this advice is unclear and may not sufficiently address the issue of implied consent as outlined above.

CrimTrac is fully aware of its obligations under Federal privacy provisions and, as such, requires the full informed consent of the individual before a check can be undertaken via the NCHRC. This provides CrimTrac with the authority to access data on a range of background information, including spent convictions, as well as satisfying strict privacy requirements.

Other relevant information - National Police Reference System (NPRS)

The National Police Reference System (NPRS), hosted by CrimTrac, provides a national view of operational policing information about persons of interest. The data provided through this system is extensive and gives law enforcement access to a diversity of data on known persons on an Australia wide basis. The NPRS is currently being used by most States and Territories, with 46,000 police users. The final rollout of the system is to occur in July 2009.

The NPRS makes available an extended set of national information identified as necessary to support local police which is intended to provide:

- Improved identification of suspects and previously unknown people of interest, through the provision of personal identity information, including physical description data and photographs (if available); and
- An alert to field officers and investigators about a person's propensity for violence and relevant information regarding warnings, warrants, family violence, bail and offence history (offender processing and criminal history), also if currently wanted by police nationally or reported as an active missing person or escapee.

The Report of the *Parliamentary Joint Committee on the Australian Crime Commission - Inquiry into the future impact of serious and organised crime on Australian society* which was released on 19 September 2007 made a number of recommendations that impact on CrimTrac. The committee saw:

> *"...much value in continuing to improve the information available to LEAs to assist their operations in an increasingly complex crime environment, and considers the MNPP [NPRS] to be the most appropriate database on which new datasets could be held".*

Recommendation 17 of that report relates to the National Police Reference System (NPRS).

"*The committee recommends that CrimTrac be funded to examine the legislative, administrative and technical aspects to allow the inclusion of additional datasets to the Minimum Nation-wide Person Profile [NPRS]; particular consideration should be given to Aviation Security Identification Cards, Maritime Security Identification Cards, explosives licences and ammonium nitrate licences (8.25)"*

The NPRS has the technical capacity to include additional information sets on Aviation Security Identification Cards (ASIC), Maritime Security Identification Cards (MSIC), explosives licences and ammonium nitrate licences, should the Commonwealth, as owners of ASIC and MSIC information, and jurisdictions, as owners of information relating to explosives and ammonium nitrate licences agree to share such information. The use of the NPRS in this manner would also require the approval of the CrimTrac Board of Management as owners of the system.

Essentially if this information was held on the system, it would likely operate in the following way – A holder of an ASIC or MSIC licence (or card, licence, permit or authorisation for which a national security background check was necessary), would be flagged in the system. If that person came to police attention in the NPRS system, such as through a change to their offence history, then, AusCheck could be notified of the change in the licensee's circumstances. The Governments response to the parliamentary Joint Committee is pending.

Jeff Storrer

Acting CEO

CrimTrac