Privacy Impact Assessment

Proposed CrimTrac and Australian Crime Commission Merger

Table of Contents

1. Introduction

CrimTrac and the Australian Crime Commission (ACC) are two of Australia's national law enforcement bodies, created to provide police with access to national criminal information and intelligence. Both agencies are shared national assets that embody Australia's cooperative response to crime, through their strong linkages with police agencies across Australia.

The changing nature of criminal and national security threats poses an ever-increasing challenge for both law enforcement and intelligence agencies. Criminal threats are becoming more complex and pervasive than ever before across the spectrum of serious and organised crime. Law enforcement and intelligence agencies have a growing requirement for accurate and up-to-date information to inform decision making processes in their everyday work.

At the same time, there is currently limited interoperability and information sharing between Australia's criminal information and criminal intelligence assets. This limits the ability to support police and other key stakeholders to manage crime-related risks.

Both the ACC and CrimTrac recognise that they have vulnerabilities that are the other agency's strengths. For example, the ACC has sophisticated analytic capability for providing intelligence, but has full connectivity to only 20 per cent of national criminal information data holdings. CrimTrac has extensive linkages with every police agency and informs 90 per cent of everyday on-the-ground police operations, but its *ICT Blueprint for National Police Information Sharing 2014-2018* recognises the need for analytic capability across its data to better support everyday policing.

The purpose of the merger is to ensure that Australia is using its national law enforcement information and intelligence capabilities as effectively as possible to support police to protect the community.

The merger would deliver benefits for law enforcement and national security, including streamlined access to information and intelligence and shared strategic insight and situational awareness.

Combining the existing resources, capabilities and expertise of these agencies provides a significant opportunity to overcome risks to the national policing environment presented by the current limited connectivity between these key national intelligence and information agencies.

Privacy impact

The *Privacy Act 1988* applies to acts and practices of agencies with certain exceptions (s 7). The exceptions include acts and practices of the ACC (s 7(1)(a)(iv)) and acts and practices of other agencies in relation to a record that originated with, or was received from, the ACC (s 7(1)(h)).

While merging CrimTrac into the ACC means that information currently held by CrimTrac will no longer be subject to the Privacy Act, this information will become subject to the same robust accountability, oversight and information protection mechanisms that protect the sensitive information that the ACC currently handles.

The merger will not impact on the rights individuals have to access and correct their personal information held by the ACC through the *Freedom of Information Act 1982*.

Key findings

The assessment ultimately finds that, while merging CrimTrac into the ACC will mean it will no longer be subject to the Privacy Act, this will not result in a diminution of protection for the personal information currently held by CrimTrac.

This assessment takes into account the purpose of the merger, the nature of CrimTrac's existing operating model, the way CrimTrac currently handles information (which will continue following a merger), and the new protections that will apply to this information following a merger.

The assessment recommends that the agencies develop and publish an information handling protocol, in consultation with the Office of the Australian Information Commissioner, outlining how information will be handled by the merged agency.

2. Threshold Assessment

The project will result in a shift of functions (and associated information) from CrimTrac, which is an agency that is subject to the Privacy Act, to the ACC, which is not subject to the Privacy Act.

As merging the agencies will involve a change in the status of personal information under the Privacy Act, AGD, the ACC and CrimTrac have prepared a Privacy Impact Assessment (PIA) to analyse the impact the merger will have on the protection of that information.

3. Scope

This PIA assesses the privacy impacts of merging the ACC and CrimTrac and will assist in analysing the possible impacts on individuals' privacy in a merged agency and make recommendations for avoiding, minimising or mitigating negative privacy impacts.

4. General Information

CrimTrac's existing operating model

Police agencies collect a variety of national policing information in the ordinary course of their business. This can include personal and sensitive information, such as names, addresses, dates of birth and criminal history information, including names of victims and perpetrators of child sex abuse.

Except for a few cases outlined below, CrimTrac is not a primary 'collector' of information. Its role is to facilitate the sharing of this information between police, for national policing and law enforcement purposes. As such, CrimTrac is largely a conduit, providing the infrastructure through which police agencies can access information held by other jurisdictions and share that information between jurisdictions, assisting them to form a more complete national picture of criminal information. For example, information in CrimTrac systems enables police to check whether a person arrested in their jurisdiction has previous convictions in another jurisdiction. (see '6. Overview of Information Flows' below for further detail).

Information holdings

Information shared through CrimTrac systems generally continues to be held in police systems, and those systems will continue to be subject to information protection and access laws that apply to the originating agency. This is despite CrimTrac being a holder of this information for the purpose of relevant Commonwealth legislation (including Privacy and freedom of information legislation). CrimTrac does not currently have the authority to vet or alter personal information contained in police records.

This situation creates practical challenges that CrimTrac has had to manage with respect to upholding privacy principles. Jurisdictions consider information provided to CrimTrac belongs to them, despite Commonwealth legislation allowing individuals to bypass owning agencies to, for example, request access to this information. Corporate staff do not have access to police information holdings and CrimTrac staff are generally not authorised to access police information in CrimTrac systems. From a practical perspective, any changes CrimTrac may make to information in its systems would not flow into the systems of the agency providing that information.

In broad terms, CrimTrac has respected the position that jurisdictions have primary ownership of their information. In practice, CrimTrac defers to the police agency that collected a particular piece of information for taking any specific privacy action, such as correction of information.

Exception - CrimTrac information

There is very little personal information shared through CrimTrac systems that is not held by the originating organisation. Key exceptions to this are:

- The Australian Cybercrime Online Reporting Network (ACORN): members of the public provide personal information directly to the ACORN. However, in doing so, users must provide consent to the way in which this information is handled. As with the other systems it provides, CrimTrac does not access or amend the information held in the ACORN – it merely provides the infrastructure. The ACC is the 'administrative user' of

the ACORN, and it performs this role. These arrangements will continue following a merger (see '6. Overview of Information Flows' below).

- National Child Offender System: The majority of jurisdictions rely on CrimTrac's NCOS to store child offender information. This system is subject to specific legislation enacted in each state and territory under the Australian Child Protection Offender Reporting scheme, which includes specific rights and restrictions around access to information.

- National Automated Fingerprint Identification Service: The majority of jurisdictions rely on NAFIS to store fingerprint and palm print information relating to known individuals. This system will continue to operate in the same way following a merger. The disclosure and use of information in NAFIS is limited to the identification of persons of interest and solving major crimes.

- National Police Checking Service (NPCS): CrimTrac receives personal information from 'Accredited Agencies' (full list here) for it to perform its NPCS, which provides police history information to police, accredited government agencies and private sector entities. This personal information is necessary so police can identify a person and provide a correct criminal history back to the requesting agency, which uses this information to assess the suitability of people applying for employment, Australian citizenship or appointment to positions of trust. The NPCS operates with the consent of the applicant.

- Immigration and border protection: CrimTrac has an arrangement with the Department of Immigration and Border Protection to assist it in discharging its responsibilities. This includes the collection of biometric information to support the Department's functions.

The table at **Attachment C** provides an overview of CrimTrac's information holdings and an indication of where information is held.

Access

With the exception of information held for its corporate functions, the information in CrimTrac systems is only accessible to its partner agencies (namely law enforcement agencies). CrimTrac staff are responsible for maintaining the systems and in most cases cannot access the information in CrimTrac systems if it is provided by a jurisdiction. The same restrictions apply even if the information is provided directly to CrimTrac, such as from the ACORN.

Requests for access to, or correction of, information contained in CrimTrac systems are similarly referred to the agency that owns that information and can lawfully access that information. Aside from issues of propriety and authority around CrimTrac staff amending another agency's information, any correction that were to be made to information in CrimTrac systems would not be reflected in the originating jurisdiction's systems unless CrimTrac is the sole holder of the information. Correcting information in police systems, on

the other hand, allows that correction to flow through CrimTrac systems and be reflected nationwide.

Post-merger handling of CrimTrac information

One of the key issues that states and territories raised during consultation on the merger was that they must retain 'ownership' of the information they provide through CrimTrac's systems and that the integrity of that information must be preserved. In this context, the current practices and procedures that underpin CrimTrac's handling of personal information will largely continue to apply within the merged agency.

Jurisdictional privacy protections

Although CrimTrac information will no longer be subject to the Australian Privacy Principles (APPs), individuals will continue to be able to access and correct records relevant to them under privacy mechanisms in their state or territory. While CrimTrac may extract information held in CrimTrac's systems (which may include personal information) for ACC intelligence purposes, the underlying information will not be altered by the merged agency and it will continue to be subject to state and territory privacy regimes.[1] These regimes will continue to govern the management, collection, use, disclosure, quality, integrity, access and correction of this information (see **Attachment A** for a comparison of jurisdictions' information privacy principles with the APPs).

This will ensure that personal information stored on CrimTrac systems will continue to be subject to appropriate privacy protection, even though the merged agency will not be subject to the Privacy Act or its equivalents in jurisdictions. For example, this would mean that the agency would continue to refer an individual to the originating police agency for any requests to correct information under the ACC's FOI Act obligations.

A new intergovernmental agreement, replacing the existing one that underpins the CrimTrac scheme, will be negotiated and signed with jurisdictions. It will also ensure that the integrity and ownership of CrimTrac-type information will be maintained in the merged agency.

Protections under the Australian Crime Commission Act 2002

Current ACC Act Protections

As CrimTrac will merge into the ACC, the information in its holdings will be subject to the information protection mechanisms that currently apply to the ACC under the *Australian Crime Commission Act 2002* (ACC Act).

[1] South Australia and Western Australia do not have Privacy legislation. South Australia Police are subject to the *Information Privacy Principles Instruction*, issued in Cabinet Administrative Instruction 1/89 (most recently reissued 16 September 2013). Western Australia police treat information in accordance with a Privacy Statement, available at <https://www.police.wa.gov.au/Privacy>.

The ACC Act contains strict limitations on the dissemination of any information in the ACC's possession. Under the ACC Act, the ACC can only disclose information in its possession to other government agencies if the ACC CEO considers it appropriate to do so, disclosing the information is relevant to a listed permissible purpose, and the disclosure would not be contrary to a Commonwealth, state or territory law (section 59AA).

In addition to these requirements, the ACC can only disclose information to bodies corporate that have been prescribed by the regulations and where the body has undertaken in writing not to use or disclosure that information except for the purpose it was shared with them (section 59AB).

Using or disclosing information in the ACC's possession in breach of these provisions is an offence punishable by up to 2 years imprisonment. Arguably, this provides greater protection to ACC information than that currently afforded to CrimTrac-held information under the Privacy Act.

Proposed additional protections

The *Australian Crime Commission Amendment (National Policing Information) Bill 2015* (which would implement the proposed merger) will further restrict the disclosure of CrimTrac-type information by the merged agency, requiring ACC Board approval before disclosure is made to a body that is not an agency represented on the Board. The ACC Board comprises all police commissioners, the Secretary of the Attorney-General's Department, the Commissioner of the Australian Border Force, the Director General of ASIO, the Chair of the Australian Securities and Investments Commission and the Commissioner of Taxation. This will ensure close scrutiny of the release of any information to non-law enforcement bodies.

Further, while the ACC is not subject to the Privacy Act, it is an agency that deals with a diverse range of sensitive information as part of its core business and is very experienced in ensuring that that information is appropriately handled and secured.

As with the other types of sensitive information it holds, the ACC will also put technical and administrative mechanisms in place to ensure that 'CrimTrac' type information continues to be collected, used and stored securely.

This will ensure that, even though it is not subject to the restrictions in the Privacy Act, the merged agency will only disclose information (which may include personal information) in very limited circumstances.

Oversight

In line with its exemption from the Privacy Act, the ACC is not subject to oversight by the Office of the Australian Information Commissioner. This means that individuals will no longer be able to access the individual remedies currently provided by the OAIC, such as compensation and enforceable undertakings in relation to CrimTrac-type information.

However, the ACC is already subject to a robust accountability framework. Should an individual have a complaint about how the ACC deals with their personal information, depending on the nature of that complaint, the ACC's conduct can be examined by:

- the Commonwealth Ombudsman – who can investigate complaints about the ACC's actions and decisions to see if they are wrong, unjust, unlawful, discriminatory or just plain unfair
- the Integrity Commissioner – who can investigate allegations of corrupt activity by current and former staff of the ACC, and
- the Parliamentary Joint Committee on Law Enforcement – whose role is to monitor and review the ACC's performance.

In addition to this, the Commonwealth Ombudsman can provide similar remedies to the OAIC if the actions of the ACC are found to be unreasonable, unlawful, unjust or discriminatory. These remedies can include financial compensation, directing the agency to make an apology or directing a change to agency policy.

These bodies have extensive expertise on the ACC, its functions, statutory regime and secrecy provisions, making them the most appropriate bodies to monitor the ACC's compliance with its obligations under the ACC Act.

The ACC also has an effective complaints handling process that ensures individuals can make complaints about the ACC and have its conduct investigated. The ACC has an internal Integrity Assurance Team that receives and considers both internal and external complaints involving the ACC and/or ACC staff.

Depending on the nature of the complaint, the ACC has a number of policies and procedures in place to deal with the complaint, including appropriate review processes.

Staff who are seconded to or work with the ACC under task force arrangements are in most circumstances also subject to their home agencies' 'professional standards' arrangements—subject to agreements between their agency and the ACC.

This change in CrimTrac oversight is appropriate given the sensitive nature of ACC operations. The ACC is already subject to a strict system of oversight and accountability that is specifically designed to ensure that the ACC exercises its powers appropriately while maintaining the appropriate balance between secrecy and accountability.

Improved Information sharing

While CrimTrac and the ACC are both 'enforcement agencies' under the Privacy Act, cultural and technical barriers currently prevent and obstruct their capacity to share important enforcement quickly and easily. This inhibits the development of an accurate understanding of the national policing landscape and is one of the key reasons jurisdictions have unanimously agreed to pursue a merger.

Therefore, to achieve the policy aims of the merger and break down the cultural barriers that currently prevent the effective flow of enforcement information between CrimTrac and the ACC, it is critical that the entire agency be subject to the same overarching information oversight regime.

Following the merger, if CrimTrac-type information or functions were carved out of the ACC's Privacy Act exemption, it could potentially perpetuate the cultural issues that currently prevent CrimTrac from legitimately sharing information with the ACC in a timely manner.

While these disclosures would always be for law enforcement purposes (and would therefore fit within the APPs), having to demonstrate this each and every time the merged agency shares information between different functions would be time consuming, resource intensive and could prevent the merged agency from accessing the information it needs to provide time-critical intelligence to police. In essence, this approach would maintain the information silos that the merger seeks to break down by perpetuating the existing connectivity and information sharing issues currently faced by the agency and preventing front line officers from having the most up-to-date and comprehensive information and intelligence. Removing these barriers is not expected to have an adverse impact on individual privacy.

5. Overview of Information Flows – pre- and post-merger

Most CrimTrac systems operate under similar processes for the collection, use and storage of personal information and access and correction requirements. The exception to this is the ACORN, which requires the providers of information to consent to CrimTrac using the information.

Most CrimTrac systems

Collection: Information is collected by police and provided by police to the CrimTrac system. This can include personal and sensitive information pertaining to individuals. It is anticipated that collection will remain the same in a merged agency.

Disclosure/Use: Most CrimTrac systems are used by police as a means to identify a person of interest, to solve crime, to form a cross-jurisdictional picture of an individual or to share information across jurisdictions, among many other purposes.

The vast majority of information provided to CrimTrac is only accessible by law enforcement agencies and in most cases, CrimTrac staff cannot access the information.

It is envisaged that information stored in CrimTrac systems will be used and disclosed for similar purposes following a merger. The ACC may run a range of advanced analytics tools over the datasets for data matching, data mining and identity resolution purposes.

If the Australian Institute of Criminology is merged into the ACC, the Australian Crime and Justice Research Centre branch of ACC may, where appropriate and in a de-identified form, use CrimTrac data for its research.

As outlined above, the ACC Act continues strict limitations on the dissemination of ACC information and amendments to the Act will make these restrictions stronger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of CrimTrac information remains subject to appropriate protections.

Storage and Security: As Commonwealth Government agencies, CrimTrac and the ACC are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. CrimTrac ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of CrimTrac services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way CrimTrac and the ACC currently do.

As outlined above, the ACC is also an agency that deals with a diverse range of sensitive information as part of its core business and is very experienced in ensuring that information is appropriated secured and handled.

Individual Access/Correction: CrimTrac does not currently provide access or facilities for individuals to seek correction of personal information. The vast majority of information is not able to be accessed by CrimTrac staff and even if it was corrected in the CrimTrac database, these changes would not be reflected in state and territory databases. This would represent a continuity issue and would undermine the accuracy and reliability of information provided by CrimTrac.

An individual is directed back to the originating police jurisdiction that supplied the information to correct a record or the police jurisdiction may direct CrimTrac to do so on its behalf. The ACC will continue to be subject to the FOI Act, enabling individuals to apply to the ACC to access or correct their personal information and, where appropriate, the merged agency will adopt the same approach, directing the individual back to the originating police jurisdiction.

Australian Cybercrime Online Reporting Network

Collection: CrimTrac collects personal information from those who submit a report to the ACORN and those who provide feedback to the ACORN via the online feedback form. Sensitive information may be collected during this process.

Use/Disclosure: Use of personal information collected by the ACORN is with the consent of the person lodging the report. To enter the reporting portal, the individual must consent to the information they provide being shared with law enforcement and regulatory agencies and being stored in the ACORN facility. The information received by ACORN is used to assist law enforcement and regulatory agencies investigate cybercrime.

As discussed above, the ACC Act contains strict limitations on the dissemination of ACC information to government bodies and bodies corporate. The amendments to the ACC Act would place further restrictions on the dissemination of national policing information following a merger. This will ensure that dissemination of ACORN information remains subject to appropriate protections. It is envisaged that current use and disclosure arrangements will continue post-merger.

Storage and Security: CrimTrac and the ACC are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. CrimTrac ICT security is addressed is addressed in the same way as all other CrimTrac systems – through appropriate physical, technical and administrative controls. A merged agency will continue to store and secure information in the same way CrimTrac and the ACC currently do.

Access: Authorised CrimTrac staff are able to access the ACORN data. The ACC, the Australia Competition and Consumer Commission, the Australian Communications and Media Authority, the Australian Cyber Security Centre and the Office of the Children's E-Safety Commissioner are also able to access data provided to the ACORN. It is envisaged that access to the ACORN will remain the same in a merged agency.

Individual Access/Correction: Individuals may currently apply to CrimTrac for access to its information holdings for personal information relating to them. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system where appropriate.

For more information, please see Attachment B

6. Privacy Impact Analysis

Privacy Risks

Assessing the privacy risk of this proposal involves comparing the conditions under which CrimTrac currently holds information with the conditions under which it will be held by the ACC.

Comparison of Commonwealth, state and territory privacy principles

Information in CrimTrac's systems is currently subject to the Australian Privacy Principles. The agencies that primarily collect the information and provide it to CrimTrac, such as state

and territory police, are also subject to privacy principles at the state, territory and Commonwealth levels.

Attachment A provides a high level comparison between Commonwealth and state and territory privacy principles. Privacy principles in South Australia and those that apply to Western Australia Police are not legislated.

The primary collectors of CrimTrac information will continue to be subject to privacy principles regarding:

- open and transparent management of information (APP 1)
- collection of personal information, including notification where information is collected (APPs 3 and 5)
- appropriate use of personal information (APP 6)
- protecting the integrity of personal information (APPs 11 and 12), and
- providing individuals with rights of access and correction through providing agencies (APPs 12 and 13)

Although these principles will continue to apply to primary collectors, they will not be binding on information actually stored in CrimTrac systems within the merged agency.

This will not practically impact on individuals' ability to access and correct their information, as these rights will be exercised through providing agencies. Currently CrimTrac staff cannot access police information and any corrections that were to be made by CrimTrac would not be carried across to the originating systems. CrimTrac does not correct jurisdictional data for this reason.

The ACC's current robust arrangements for protecting the security, quality and integrity of information will not lessen the protection currently provided by APPs 11 and 12.

Practices around collection and use of information will not change – this will continue to be primarily for law enforcement purposes by law enforcement agencies.

Although it will no longer be bound to do so, the merged agency will ensure continuity of transparency around CrimTrac information (as per APP 1) by publishing an information handling protocol.

For other principles, there is inconsistent coverage across jurisdictions, including:

- anonymity or pseudonymity (APP 2)
- dealings with unsolicited information (APP 4):
- restrictions on direct marketing (APP 7)
- ensuring overseas recipients do not breach APPs (APP 8), and
- restrictions on the adoption, use and disclosure of government related identifiers by organisations (APP 9).

Individuals will not have consistent recourse to these principles but this is unlikely to have a significant impact on the level of protection afforded to CrimTrac information.

CrimTrac mostly receives information from police and other agencies in connection with its law enforcement support functions. This will not change following a merger.

CrimTrac does not deal directly with individuals, except for ACORN (in accordance with its own privacy policy), NPCS and for its own corporate matters. Neither CrimTrac nor the ACC engage in any direct marketing. These matters are unlikely to change.

CrimTrac has arrangements with international bodies that assist law enforcement agencies maintain the safety of the Australian community. CrimTrac would continue to only disclose information pursuant to these arrangements consistent with the APP's, unless:

- the individual has consented;
- the individual would reasonably expect, or has been told, that information of that kind is usually passed to those individuals, bodies or agencies;
- it is required or authorised by law;
- it will prevent or lessen a serious and imminent threat to somebody's life or health; or
- it is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of public revenue.

Other Potential Risks

There may also be risks in specific scenarios that are contemplated by the Privacy Act. For example, CrimTrac operates the National Missing Person Victim System. Section 16A(2) of the Privacy Act allows the Privacy Commissioner to make rules relating to the collection, use or disclosure of missing person information. The Privacy (Persons Reported as Missing) Rule 2014 has been made under this provision, and among other things, requires an APP entity to respect any wishes of missing persons of which they are aware in using or disclosing information about them. The ACC would not be bound by this requirement.

Mitigation measures

Managing privacy risks

Despite the assessment that the transition to a merged agency is unlikely to detract from the protection of incoming CrimTrac information, the agencies will give specific consideration to how best to protect personal information, particularly biometric information.

As part of this process, consideration will be given to any unforeseen consequences that may arise due to the transition from the Privacy/APP regime to the ACC Act regime. Information handling arrangements will be monitored on an ongoing basis after the merger.

Specific consideration will also be given to how the merged agency will deal with certain scenarios, such as missing persons (as detailed above). This consideration will begin with a presumption that any current protections will continue unless it would impede the activities of the merged agency or law enforcement.

Greater ACC access to CrimTrac information

The key difference in what would happen to CrimTrac information post-merger relates to the greater access by ACC to this information and development of subsequent intelligence products using CrimTrac information.

As with the other types of information it collects, the ACC will put administrative and technical measures in place to ensure that personal information is accessed, used and stored appropriately.

For example, as part of its statutory functions, the ACC currently maintains a national database of criminal information and intelligence known as ACID (Australian Criminal Intelligence Database).

The ACID system comprises information and intelligence from various law enforcement agencies, including State agencies.

Like the CrimTrac model, the integrity of the data contained in ACID is maintained by the originating agency and access to the information is controlled by a layered approach including agency data sharing controls (i.e. who can see the information), restricted document controls (i.e. what information can be seen), document classifications, user clearances and network security ratings.

The ACC's involvement in ACID (including ACC access to information in the system) is governed by a detailed MOU.

Where, as part of its additional functions, the ACC accesses information in ACID, within the terms of the MOU, any subsequent dissemination is governed by the strict dissemination provisions contained in the ACC Act, which adds an additional layer of information protection.

The ACC envisages that its experience with the ACID system can be utilised with CrimTrac systems.

Additional Considerations

The ACC Act currently contains strict information sharing provisions that apply to 'ACC information' as outlined above. 'ACC information' is broadly defined to mean information that is in the ACC's possession. Given the breadth of this definition, following a merger, CrimTrac information and data holdings would become 'ACC information' for the purposes of the Act.

The Australian Crime Commission (National Policing Information) Bill would amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information following a merger as outlined above.

Further, while the ACC does not fall within the Privacy Commissioner's jurisdiction, it is subject to a robust accountability framework should it mishandle personal information, as outlined above.

7. Recommendations

1. ***The agencies should ensure that appropriate safeguards are in place to protect CrimTrac personal information, including in relation to:***
    - ***Collection: As collection practices will not change, the ACC should continue to apply the rules CrimTrac currently does regarding how it receives information from partner agencies and the public to the extent possible. In particular, the agency should substantially continue the conditions and protections that apply to information collected through the ACORN and for the NPCS.***
    - ***Storage, security and use/disclosure: The ACC should implement strict physical, technical and administrative controls on access to CrimTrac information to ensure that personal information is only accessed by those with a business need and used and disclosed as appropriate. These controls should focus on restricting access to those within the ACC that have a need to know, but should also take account of the need to ensure appropriate intelligence staff can freely access this information in line with the objectives of the merger.***
    - ***Access and correction: The ACC should continue to ensure that appropriate access and correction opportunities are afforded to individuals by ensuring staff refer requests to the appropriate originator of information flowing through CrimTrac systems.***
    - ***Other specific privacy scenarios: to the extent possible, the ACC should adopt other conditions required of APP entities in relation to personal information where it is appropriate to do so and does not impair their functions. For example, the provisions around missing persons as provided by the* Privacy (Persons Reported as Missing) Rule 2014.**
2. ***To ensure transparency and continuity of protection of CrimTrac information by the merged agency, including on the matters referred to in recommendation 1, the ACC should develop and publish an information handling protocol that addresses the way in which the agency will treat personal information. This protocol should reflect the standards set out in the Australian Privacy Principles and be developed in consultation with the Office of the Australian Information Commissioner.***
3. ***ACC staff should be appropriately trained to ensure they are able to comply with the information handling protocol***

Attachment A - Commonwealth Privacy Principles vs State and Territory privacy principles

	Consideration of personal privacy		Collection			Dealings				Integrity		Access	
	Open and transparent management (APP 1)	Anonymity and pseudonymity (APP 2)	Collection of solicited personal info (APP 3)	Dealing with unsolicited personal info (APP 4)	Notification of collection (APP 5)	Use or disclosure of personal info (APP 6)	Direct marketing (APP 7)	Cross border disclosure of personal info (APP 8)	Adoption, use or disclosure of govt related identifiers (APP 9)	Quality of personal information (APP 10)	Security of personal information (APP 11)	Access to personal information (APP 12)	Correction of personal information (APP 13)
ACT *Information Privacy Act 2014*	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
NSW *Privacy and personal information protection Act 1998*	Some – privacy management plans (s 33), also transparency under s 13	No	Yes (ss 8–9)	No	Yes (s 10)	Yes (s 17–19)	No	No	No	Yes (s 11)	Yes (s 12)	Yes (s 14)	Yes (s 15)
NT *Information Act*	Yes (Sched 2, IPP 5)	Yes (Sched 2, IPP 8)	Yes (Sched 2, IPP 1, IPP 10 re sensitive information)	No	Yes (Sched 2, IPP 1)	Yes (Sched 2, IPP 2)	No	Yes (Sched 2, IPP 9)	Yes (Sched 2, IPP 7)	Yes (Sched 2, IPP 3)	Yes (Sched 2, IPP 4)	Yes (s16, Sched 2 IPP 6)	Yes (s16, Sched 2 IPP 6)
Queensland *Information Privacy Act 2009*	Yes (Sched 3, IPP 5, also IPP 2)	No (only health agencies)	Yes (Sched 3, IPPs 1-3)	No	Yes (Sched 3, IPP 2, but only for info collected from individual)	Yes (Sched 3, IPPs 9-11)	Yes (Sched 3, IPP 11(4))	No	No	Yes (Sched 3, IPP 7)	Yes (Sched 3, IPP 4)	Yes (Sched 3, IPPs 6, 8)	Yes (Sched 3, IPP 7)
South Australia No legislation *(Information Privacy Principles Instruction)*	Some - reporting to Privacy Committee	No	Yes (4(1)-(3))	No	Yes (4(2))	Yes (4(7)-(10))	No	No	No	Yes (4(9))	Yes (4(4))	Yes (4(5))	Yes (4(6))
Tasmania *Personal Information Protection Act 2004*	Yes (Sched 1, PIPP 5)	Yes (Sched 1, PIPP 8)	Yes (Sched 1, PIPP 1, PIPP 10 re sensitive information)	No	Yes (Sched 1, PIPP 1)	Yes (Sched 1, PIPP 2)	No	Yes (Sched 1, PIPP 9)	Yes (Sched 1, PIPP 7)	Yes (Sched 1, PIPP 3)	Yes (Sched 1, PIPP 4)	Yes (Sched 1, PIPP 6)	Yes (Sched 1, PIPP 6, s 17A)
Victoria *Privacy and Data Protection Act 2014*	Yes (Sched 1, IPP 5)	Yes (Sched 1, IPP 8)	Yes (Sched 1, IPP 1, IPP 10 re sensitive information)	No	Yes (Sched 1, IPP 1)	Yes (Sched 1, IPP 2)	No	Yes (Sched 1, IPP 9)	Yes (Sched 1, IPP 7)	Yes (Sched 1, IPP 3)	Yes (Sched 1, IPP 4)	Yes (Sched 1, IPP 6)	Yes (Sched 1, IPP 6)
Western Australia No legislation (WAPol Privacy Statement)	Yes	No	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes

Attachment B – overview of systems

Australian Cybercrime Online Reporting Network	
Collection	CrimTrac collects personal information from those who submit a report to the ACORN and provide feedback to the ACORN via the online feedback form. Sensitive information may also be collected if it is provided in the report or feedback to the ACORN. As a crime reporting tool, ACORN has the capacity to collect personal information about an alleged suspect. Use of personal information collected by the ACORN is with the consent of the person lodging the report. To enter the reporting portal, the individual must consent to the information they provide being shared with law enforcement and regulatory agencies and being stored in the ACORN facility. The majority of information collected is regarded as information solicited by the collecting agency for the purposes of APP 3. However, where information about an alleged suspect is provided by a submitting party, it is recognised that this information is likely to be provided without consent. It is anticipated that this information will continue to be collected in this way. - Personal details collected include name, DOB, gender, IPP address
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is also an agency that deals with a diverse range of sensitive information as part of its core business. It is very experienced in ensuring that that information is appropriately secured and dealt with.

	As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Use /Disclosure	Currently: • ACORN is currently subject to the Privacy Act 1988 • Primary purpose - To assist law enforcement and regulatory agencies investigate cybercrime. • Secondary purpose - Information is de-identified to prevent the use of personal information for secondary purposes (intelligence purposes). • Consent given or de-identified personal information provided to other countries We envisage that ACORN information will be used and disclosed for similar purposes following a merger. Further, the ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of ACORN information remains subject to appropriate protections.
Access	CrimTrac - authorised users based on their role. ACC ACCC ACMA ACSC Children's e-safety office.

	It is envisaged that access to this system will remain the same in a merged agency.
Individual Access/Correction	Individuals may currently apply to CrimTrac for access to its information holdings for personal information relating to them. This can be done by contacting either the Privacy Officer at 02 6268 7639 or via privacy@crimtrac.gov.au. While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Automated Fingerprint Identification System	
Collection	Information is collected by police and provisioned by police to the system. This includes sensitive and Personal Information pertaining to known individuals. It also includes the following information from unknown individuals. - Fingerprints, Palm image - Person Details such as Name, DOB, gender etc. - Person History such as wanted, charges It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is also an agency that deals with a diverse range of sensitive information as part of its core business. It is very experienced in

	ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/Disclosure (APP6)	– Police Jurisdictions – Immigration and Border Force • Primary purpose - Used by police as a means of positively identifying a person of interest (identity resolution) • Secondary purpose - Used to assist police solve major and minor crimes
Anticipated Use/Disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. In addition, the ACC may run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The Australian Crime and Justice Research Centre branch of ACC may, where appropriate and in a de-identified form, use CrimTrac data for its research. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of NAFIS information remains subject to appropriate protections.
Current Access	Police Delegated Immigration and Border Force staff

Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that Police and delegated DIBP staff will retain access to NAFIS following a merger.
Correction	CrimTrac does not currently provide access or facilities for individuals to seek correction of personal information held in the NAFIS – an originating police jurisdiction may correct (update) a NAFIS record, or direct CrimTrac to do so on its behalf. While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Criminal Investigation DNA Database	
Collection	Information is collected by police and provisioned by police to the system. Information collected includes sensitive Information - Unique identifier and DNA profiles. The database contains profiles of convicted offenders, suspects, missing persons, DNA profiles from volunteers and victims. It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is also an agency that deals with a diverse range of sensitive information as part of its core business. It is very experienced in ensuring that that information is appropriately secured and dealt with.

	As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/Disclosure	Provides police with the capability to conduct cross-jurisdictional DNA profile matching. The system allows for the establishment of identity but does not reveal personal details such as physical identity, age, ethnicity, race, appearance or medical conditions. The use/disclosure must be connected to the purpose of collection. The primary purpose is to provide law enforcement with a DNA matching resource to assist in the investigation of criminal offences.
Anticipated Use/Disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. In addition, the ACC will run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The Australian Crime and Justice Research Centre branch of ACC may, where appropriate and in a de-identified form, use CrimTrac data for its research. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of DNA database information remains subject to appropriate protections. Note users' have to be accredited, ACC staff will need to be accredited or belong to a laboratory.

	Any use by the ACC can only be assessed once the primary purpose of collection is clear.
Current Access	Limited number of users in police partner agencies' forensic laboratories and a number of police in QLD. Users must be accredited. DNA labs are to be accredited by NATA to present information to the court – users must undertake accreditation process (exams etc.).
Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that those currently with access to the NCIDD will continue to have access.
Correction	While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Child Offenders System – consists of the Australian National Child Offender Register (ANCOR) and the Managed Person System (MPS)	
Collection	Information is collected by police and provisioned by them to the system. Information collected includes: • Personal details such as Name, DOB, gender • Personal Alias' • ID Cards/Documents • Physical features such as hair colour, eye colour, build and complexion • Distinguishing features • Tattoos • Facial Images (photograph), indication that DNA sample has been taken • Personal History such as warnings, travel, charge, offence, court outcomes, order, bail It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and

	the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is an agency that deals with a diverse range of sensitive information as part of its core business, and is very experienced in ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/Disclosure	ANCOR enables police to register, case manage and share information about registered persons. It enables police to uphold child protection legislation in their state or territory. The MPS holds information about offenders who are charged but not convicted, or after an offender's reporting obligations have been completed.
Anticipated Use/Disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. In addition, the ACC may run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where

	otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of NCOS information remains subject to appropriate protections.
Current Access	Authorised police
Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that authorised police will maintain access to the NCOS.
Correction	While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Firearms Licencing and Registration System	
Collection	Information is collected by police and provisioned by them to the system. Information collected for this system includes: • Personal details about the licensed holder or dealer of firearms. • Biographic information such as name, dob, drivers licence • Personal History – warnings • Purpose of collection is for provision of ICT resources for policing purposes It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both

	agencies currently do. The ACC is an agency that deals with a diverse range of sensitive information as part of its core business, and is very experienced in ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/Disclosure (APP6)	Holds information about past and current firearm licence holders, licenced firearms dealers, registered, lost or stolen firearms.
Anticipated Use/Disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. In addition, the ACC may run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The Australian Crime and Justice Research Centre branch of ACC may, where appropriate and in a de-identified form, use CrimTrac data for its research. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of firearms information remains subject to appropriate protections.
Current Access	Police Agencies Approved External Agencies (ICAC, ACBP, ACC)
Anticipated	ACC access for performance of ACC functions (criminal intelligence,

Access	criminal investigation, criminology research). It is anticipated that police and approved external agencies will continue to maintain access to the NFLRS.
Correction	While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Names Index	
Collection	Information is collected by police and provisioned by them to the system. Information collected for this system includes: • Personal Information – Name, DOB, gender, alias', ID cards/documents • Sensitive Information – Fingerprint, CNI • Physical features (hair colour, eye colour, build, complexion), distinguishing features, tattoos • Personal History – warnings It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is an agency that deals with a diverse range of sensitive information as part of its core business, and is very experienced in ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure

	that information continues to be collected, used and stored securely.
Current Use/disclosure (APP6)	Primary source of information for national police checks, firearms licence holders Due to its age and platform, strategic intent is to move away from NNI.
Anticipated Use/disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. In addition, the ACC may run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The Australian Crime and Justice Research Centre branch of ACC may, where appropriate and in a de-identified form, use CrimTrac data for its research. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of NNI information remains subject to appropriate protections.
Current Access	Police jurisdictions Approved External Agencies (ICAC, ASIC, ACBP, ACC)
Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that police and approved external agencies will maintain access to the NNI.
Correction	While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue

	to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Police Checking Service Support System (NSS) - The NSS is the tool that facilitates the collection, use, storage and disclosure of information relevant to a National Police History Check.	
Collection	CrimTrac collects (either through Accredited Organisations or Police Agencies) the following information specifically for the purpose of the NPCS: • the Applicant's surname and given names(s), and all names under which the Applicant is or has been known; • the Applicant's date and place of birth; • the Applicant's sex; • the Applicant's residential address(es) for the past five years; • the Applicant's driver's licence details and/or firearms licence details; • the position title, occupation, or entitlement being sought by the Applicant; • the Applicant's signature; and • the proposed place of work and whether contact with children or vulnerable groups such as the elderly is likely. The information collected by CrimTrac via its Accredited Organisations is input into the NSS by the collecting Organisation. It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems,

	infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is an agency that deals with a diverse range of sensitive information as part of its core business, and is very experienced in ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/Disclosure	The primary purpose of collection of information in the NSS by CrimTrac is to provide individuals (employer's/decision makers) with access to police/conviction history information with the consent of the individual. Typically use and disclosure of information occurs at several stages: • CrimTrac uses the information for potential matches; • CrimTrac discloses the information to Police Agencies for matching and information retrieval; • Police Agencies use the information for matching; • Police Agencies disclosure the information to CrimTrac for collation into a NPHC result; • CrimTrac discloses the information to the requesting agency; • the requesting agency discloses the information to the relevant employer/decision maker/individual.
Anticipated Use/Disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. ACC may also run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The

	Government intends to amend the ACC Act to insert further restrictions on the dissemination of nationally coordinated criminal history checks following a merger. The ACC may only disclose information from a nationally coordinated criminal history check where otherwise consistent with other Commonwealth, state and territory laws, and within any restrictions or conditions determined by the Board. This will ensure that disclosure of national criminal history check information remains subject to appropriate protections.
Current Access	- State and Territory Police Agencies; - The AFP; - CrimTrac; and - CrimTrac accredited organisations in accordance with the Terms of Service for controlled access by duly Accredited Organisations to the National Police Checking Service (the Terms of Service).
Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that state and territory police agencies, the AFP, CrimTrac and CrimTrac accredited organisations will maintain access in a merged agency.
Correction	The position taken by CrimTrac in respect to its information sharing solutions for law enforcement is that any request to correct personal information of this nature must be directed to the police agency that input the information. While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Vehicles of Interest	
Collection	Information is collected by police and provisioned by them to the system. Information collected includes: • biographical information on police officers attending an incident • Name, DoB, Gender, Rank, NEPI login

	It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is an agency that deals with a diverse range of sensitive information as part of its core business, and is very experienced in ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/disclosure	Records and tracks stolen and wanted vehicles and vehicle parts. Stores information on police officers Links with Austroads NEVDIS which holds vehicle registrations, vehicle operators and driver licences
Anticipated Use/Disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. In addition, the ACC may run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The Australian Crime and Justice Research Centre branch of ACC may, where appropriate and in a de-identified form, use CrimTrac data for its research. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's

	possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of NVOI information remains subject to appropriate protections.
Current Access	Police Approved External Agencies (CMC, ACBP)
Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that police and approved external agencies will maintain access to the NVI.
Correction	While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Missing Person Victim System (NMPVS)	
Collection	Information is collected by police and provided by them to the system. Information includes: • Disaster Victim Identification (DVI) – information may be gathered from interviews with family and friends e.g. dental records, medical records and x-rays and DNA • Long Term Missing Persons (LTMP) (3-6mths) – information collected in response to LTMP is for the purpose of resolving that LTMP (using an Anti-Mortem form) • Unidentified Human Remains (UHR)- information is collected using a post-mortem form NMPVS may collect information obtained through a forensic procedure (fingerprint or DNA sample) Information is electronically tagged according to one of the three

	purposes it was collected. It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is an agency that deals with a diverse range of sensitive information as part of its core business, and is very experienced in ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/Disclosure	Assist police users to undertake national searches on long-term missing persons, unidentified human remains and disaster victim identification. Maintain a LTMP and DVI register for police Ability to undertake automated national search on LTMP and UHR NZ Police are able to reconcile DVI data, but do not have access to LTMP/UHR cases Disclosures currently authorised by relevant jurisdiction.
Anticipated Use/Disclosure (ACC)	We envisage that information on this system will be used and disclosed for similar purposes following a merger. In addition, the ACC may run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets.

	The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of NMPVS information remains subject to appropriate protections.
Current Access	Police Agencies, NZ Police (DVI cases only) and expert organisations. Access to DVI cases will be managed according to permissions granted by the relevant lead agency.
Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that police agencies, NZ Police (DVI cases only) and expert organisations will continue to have access to the NMPVS in the same way they currently do.
Correction	The position taken by CrimTrac in respect to its information sharing solutions for law enforcement is that any request to correct personal information of this nature must be directed to the police agency that input the information. CrimTrac currently has a responsibility to meet the wishes of a person reported as missing if that person communicates that they don't want to be found – but ACC doesn't, as it's not an APP Entity. However, while the ACC does not have a legal obligation, it should continue to adopt this position where possible. While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.
National Police Reference System	

Collection	Information is collected by police and provided by them to the system. Information includes: • Personal Information – Name, DOB, gender, alias', ID cards/documents, addresses and historical data • Sensitive Information – Fingerprint, CNI • Physical features (hair colour, eye colour, build, complexion), distinguishing features, tattoos • Personal History – warnings, warrants, orders It is anticipated that this information will continue to be collected in this way.
Storage/Security	As Commonwealth Government agencies, the ACC and CrimTrac are required to follow the Protective Security Policy Framework (PSPF), and the guidelines of the Information Security Manual (ISM) for the provision of ICT Security. ICT Security is addressed through the provision of appropriate physical, technical and administrative controls. These controls, identified through a structured risk assessment process, are designed to maintain the confidentiality, integrity, and availability of services, through protection of ICT systems, infrastructure and information. It is envisaged that the merged agency will continue to store and secure this information in the same way both agencies currently do. The ACC is an agency that deals with a diverse range of sensitive information as part of its core business and is very experienced in ensuring that that information is appropriately secured and dealt with. As with the other types of sensitive information it collects, the ACC should put technical and administrative mechanisms in place to ensure that information continues to be collected, used and stored securely.
Current Use/Disclosure	The National Police Reference system is used for a number of services that CrimTrac supplies to police and Approved External Agencies (including the ACC, Customs, etc.) ranging from ASIC MSIC alerts, Arson flag, Background Checking, to Biometrics at the Border. The implications to privacy are therefore varied according to usage and the legislative framework appropriate to each service and as such CrimTrac undertakes Privacy Impact Assessments on NPRS according to the usage of NPRS data.
Anticipated Use/Disclosure	We envisage that information on this system will be used and disclosed for similar purposes following a merger.

(ACC)	In addition, the ACC may run a range of advanced analytics tools over the datasets (including for data matching, data and text miners and identity resolution). In addition, tools such as Palantir and ESRI will provide network and temporal and geospatial analysis. These tools will be available for all datasets. The Australian Crime and Justice Research Centre branch of ACC may, where appropriate and in a de-identified form, use CrimTrac data for its research. The ACC Act currently contains strict limitations on the dissemination of ACC information (defined as any information in the ACC's possession) to government bodies and bodies corporate. The Government intends to amend the ACC Act to insert further restrictions on the dissemination of 'CrimTrac' type information (to be called national policing information) following a merger. Amongst other things, the ACC may only disseminate national policing information for certain defined purposes to specific bodies, where otherwise consistent with other Commonwealth, state and territory laws, and with the express agreement of the ACC Board. This will ensure that dissemination of NPRS information remains subject to appropriate protections.
Current Access	Police Approved External Agencies
Anticipated Access	ACC access for performance of ACC functions (criminal intelligence, criminal investigation, criminology research). It is anticipated that police and approved external agencies will continue to have access to the NPRS in a merged agency.
Correction	The position taken by CrimTrac in respect to its information sharing solutions for law enforcement is that any request to correct personal information of this nature must be directed to the police agency/government agency that input the information. While the ACC is not bound by the Privacy Act, it is subject to the FOI Act. The FOI Act will enable individuals to apply to the ACC to continue to access and correct their personal information held in this system. However, the ACC may refuse access to personal records where FOI exemptions apply.

Attachment C: Overview of CrimTrac information holdings and where information is held.

CrimTrac System	Summary Information	ACT	AFP	QLD	NSW	NT	SA	TAS	VIC	WA	ACC	DIBP	Comments
ABIN		SOLE	SOLE	SOLE	SOLE	SOLE	SOLE	SOLE	SOLE	SOLE	n/a	n/a	No personal information
ACORN	The jurisdictions, including ACC, are able to export data from ACORN to import into local police systems. ACORN is the source of truth, collecting reports from the public and contains personal information that cannot be verified.	Import from ACORN	Import from ACORN	Import from ACORN	Import from ACORN	Import from ACORN	Import from ACORN	Import from ACORN	Import from ACORN	Import from ACORN	Import from ACORN	n/a	
NAFIS	The National Automated Fingerprint Identification System holds information collected and provisioned by police. It includes information about known individuals as well as fingerprints, palm images and personal history	SOLE	Extract	Extract	SOLE	SOLE	SOLE	SOLE	SOLE	SOLE	n/a	Extract	
NPBI	Interface only - nothing is stored in NPBI	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
NCIDD	The National Criminal Investigation DNA Database holds information collected and provisioned by police. The system provides police with the capability to conduct cross-jurisdictional DNA profile matching but does not reveal any personal details	SOLE	SOLE	SOLE	Extract	Extract	Extract	Extract	SOLE	Extract	n/a	n/a	No personal information, only de-identified DNA profiles.
NCOS	NCOS is an extract of data from the jurisdictions (point in time). This is agency dependant as to how much they provision. Contains sensitive and personal information.	SOLE	Relies on manual data entry to and from the alerts management system (Customs)	SOLE	Manual Entry to and from COPS – Child Protection Register	SOLE	SOLE	SOLE	SOLE	SOLE	n/a	n/a	
NFID	Management tool to collate firearms Identification nationally	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	No personal information
NMPVS-DVI	Recently transitioned - likely to be SOLE source of information from a DVI. Contains personal information.	Derived	Derived	Derived	Derived	Derived	Derived	Derived	Derived	Derived	n/a	n/a	Information derived from other sources
NMPVS-MP	Recently transitioned - likely to be a mix of sole and extracted source of information from MP. Contains personal information.	Derived	Derived	Derived	Derived	Derived	Derived	Derived	Derived	Derived	n/a	n/a	Information derived from other sources
NPRS	NPRS is a point in time extract of data from the jurisdictions. This is agency dependant as to how much and when they provision. Contains personal information.	Extract	Extract	Extract	Extract	Extract	Extract	Extract	Extract	Extract	n/a	n/a	
NSS	Contains personal information provided via a consent form by the individual from AAs and jurisdictions. Retrieves information from NNI and NPRS. Currently storage of the collated information is indefinite (no deletion of data).	Derived	Derived	Derived	Derived	Derived	Derived	Derived	Derived	Derived	n/a	n/a	Information derived from other sources
(EAMS)	This is legacy system of NSS that is still holding personal information pre May 2010. Currently storage of the collated information is indefinite (no deletion of data).	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	