Australian Government
Office of the Privacy Commissioner

Level 8 Piccadilly Tower
133 Castlereagh Street
Sydney NSW 2000
GPO Box 5218
Sydney NSW 2001

P +61 2 9284 9800
F +61 2 9284 9666
privacy@privacy.gov.au

Enquiries 1300 363 992
TTY 1800 620 241
www.privacy.gov.au

ABN 13 152 473 225

Committee Secretary
Parliamentary Joint Committee on the Australian Crime Commission
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Ms Dewar

Inquiry into "*Future impact of serious and organised crime on Australian society*"

The Office of the Privacy Commissioner (the Office) would like to provide comments to the Parliamentary Joint Committee on the Australian Crime Commission (the Committee) regarding its inquiry into the "*Future impact of serious and organised crime on Australian society*" (the Inquiry). Our comments are directed in particular towards Item d of the Inquiry's terms of reference:

'*the adequacy of legislative and administrative arrangements including the adequacy of cross-jurisdictional databases, to meet future needs.'*

The Office is an independent statutory body whose purpose it is to promote and protect privacy in Australia. The Office has responsibility for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The *Privacy Act 1988* (the Privacy Act) regulates how these agencies and organisations handle personal information.

However, in terms of the Inquiry, it is important to note that the Privacy Act does not regulate intelligence agencies or the Australian Crime Commission (ACC). In addition the Privacy Act allows for exceptions to the (prescribed) use and disclosure of personal information for legitimate purposes such as law enforcement.

The Office recognises that privacy is not an absolute right. It is a right that must be balanced against other important social interests such as the safety and security of the community. The Office submits that consideration should be given to ensuring that an appropriate balance is struck between the need to collect personal information to facilitate security and safety and an individual's general right to control the collection and handling of their personal information.

Below the Office has set out some information in relation to privacy regulation in Australia that may impact on any increased sharing of information between different law enforcement agencies.

The jurisdiction of the Privacy Act

The Office considers that it is relevant to take into account the jurisdiction of the Privacy Act in terms of any proposal to expand the source and amount of personal information to be collected into law enforcement databases and access to this and any subsequent use and disclosure of that information.

The Privacy Act only regulates Australian and ACT government agencies. It does not regulate state (or Northern Territory) police services. Further, with the exception of Victoria, the state police services are not subject to any state based statutory privacy regulation although in a number of cases they are covered, at least partly, by state based privacy administrative schemes. This means that some law enforcement agencies which may have access to a cross jurisdictional database are not currently subject to statutory privacy regulation.

In terms of balancing the requirements of law enforcement activities, the Privacy Act provides an exemption for the ACC[1]. Therefore, if intelligence were to be collected from various agencies and held on an ACC database such as the Australian Criminal Intelligence Database (ACID), that information would become exempt from the coverage of the Privacy Act. Further, any record created by the ACC and later disclosed to another agency, organisation or (even an) individual would not be subject to the Privacy Act unless incorporated into that agency's databases and then only those agencies covered by the Privacy Act.

The Office is aware that new technologies have the capacity to link unrelated sources of information to create profiles of individuals. In the context of law enforcement, this could mean the aggregation of large amounts of personal information. The Office suggests that if key privacy protections such as data accuracy are not tightly observed in relation to the information held on such databases it could lead to poor decision making and have adverse impacts for individuals.

The Office believes that the Privacy Act includes exceptions that allow for intelligence collection that recognises the appropriate balance between privacy and other interests such as the safety and security of the community. Further, the Office submits that information handling practices that enhance overall data quality support better decision-making.

Therefore, the Office believes that government agencies not subject to the statutory privacy regulation should develop and implement information handling practices that incorporate principles similar to those contained within the Privacy Act. These could be adapted from the privacy principles taking into account the particular law enforcement and intelligence requirements. A similar approach has been adopted by a number of intelligence agencies by working with Inspector General of Intelligence and Security (IGIS) to develop and implement privacy guidelines.

Ideally privacy guidelines could be included as part of any memorandum of understanding or agreement between jurisdictions to access or distribute information through a database or other 'facilitation mechanism' where some of those agencies are not covered by a privacy regime similar to the Privacy Act.

[1] Under s7(1) the ACC is specifically excluded from the definition of an agency.

The Office would also like to bring to the Committee's attention the current Australian Law Reform Commission's Privacy Inquiry[2] where issues of national consistency in privacy regulation and how privacy regulation interacts with law enforcement are two of the issues being considered.

Privacy Impact Assessment and the "Four A" framework

The Office encourages agencies which are undertaking new projects, process re-engineering or system development to complete a Privacy Impact Assessments (PIA). The value of completing a PIA is that it enables agencies to identify and analyse privacy impacts during a project's design phase, which in turn assists agencies to determine the appropriate management of any negative privacy impacts and to build in privacy enhancing processes. Dealing with privacy impacts can be challenging for agencies. By conducting a PIA, agencies will be in a much better position to meet those challenges. The PIA Guide developed by the Office is available on our website at: http://www.privacy.gov.au/publications/PIA06.doc

In addition the Office has developed a framework for assessing new law enforcement powers that may impact on the handling of personal information. The framework sets out a life cycle approach to such proposals and aims to bring balance and perspective to the assessment of such measures. A copy of this framework is attached.

Summary

The Office has consistently and publicly acknowledged the public interest in maintaining the safety and security of the Australian community through effective law enforcement measures.

Further, the Office acknowledges that the policy objectives underpinning these law enforcement measures may sometimes mean diminishing the privacy protections otherwise expected by the community.

However, the Office submits that any reductions in privacy protections should reflect a proportionate response to the problem at hand, and be reasonably necessary to address that problem and can be accompanied by voluntary adherence to good privacy practices by agencies not covered by the Privacy Act.

The Office recommends that proposals to change the way in which cross-jurisdictional databases are used for law enforcement and intelligence purposes should be the result of thorough and careful assessment of the law enforcement and privacy impacts of such a decision.

Yours sincerely

Karen Curtis
Privacy Commissioner
1 August 2007

[2] http://www.alrc.gov.au/inquiries/current/privacy/

FRAMEWORK FOR ASSESSING AND IMPLEMENTING NEW LAW ENFORCEMENT AND NATIONAL SECURITY POWERS

The Office of the Federal Privacy Commissioner has developed a proposed framework for assessing and implementing new law enforcement and national security powers. The framework sets out a life cycle approach to such proposals from development to implementation and review. The aim of the framework is to bring balance and perspective to the assessment of proposals for law enforcement or national security measures with significant effects on privacy.

First, careful analysis is needed in the development phase to ensure that the proposed measure is necessary, effective, proportional, the least privacy invasive option and consistent with community expectations. This analysis should involve consideration of the size, scope and likely longevity of the problem, as well as the range of possible solutions, including less privacy invasive alternatives. The impact on privacy of the proposed solution should be analysed and critical consideration given to whether the measure is proportional to the risk.

Second, the authority by which the measure is implemented should be appropriate to its privacy implications. Where there is likely to be a significant impact on privacy, the power should be conferred expressly by statute subject to objective criteria. Generally, the authority to exercise intrusive powers should be dependent on special judicial authorisation. Intrusive activities should be authorised by an appropriately senior officer.

Third, implementation of the measure should be transparent and ensure accountability. Accountability processes should include independent complaint handling, monitoring, independent audit, and reporting and oversight powers commensurate with the intrusiveness of the measures.

Finally, there should be periodic appraisal of the measure to assess costs and benefits. Measures that are no longer necessary should be removed and unintended or undesirable consequences rectified. Mechanisms to ensure such periodic review should be built into the development of the measure. This could involve a sunset clause or parliamentary review after a fixed period.

In summary:

Analysis – is there a problem? Is the solution proportional to the problem? Is it the least privacy invasive solution to the problem? Is it in line with community expectations?

Authority – Under what circumstances will the organisation be able to exercise its powers and who will authorise their use?

Accountability – What are the safeguards? Who is auditing the system? How are complaints handled? Are the reporting mechanisms adequate? And how is the system working?

Appraisal – Are there built in review mechanisms? Has the measure delivered what it promised and at what cost and benefit?