Australian Government

Office of the Privacy Commissioner

Draft Report on the Control of Chemicals of Security Concern

Submission to COAG Review of Hazardous Materials Steering Committee

April 2008

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner ('the Office') is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988* (Cth) ('the Privacy Act'), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

About this submission

2. The Office of the Privacy Commissioner ('the Office') welcomes the opportunity to comment on the *Draft Report on the Control of Chemicals of Security Concern* ('the Draft Report'), prepared by the Steering Committee for the Council of Australian Government's (COAG) Review of Hazardous Materials. The Office acknowledges that the COAG Review of Hazardous Materials aims to establish a framework to minimise the threat to Australia from the possible use of chemicals for terrorist purposes.
3. The comments below are limited to issues related to the handling of personal information.
4. As noted throughout this submission, the Office would welcome the opportunity for further consultation in regard to matters that may affect personal information.

The Privacy Act

5. The Privacy Act contains eleven Information Privacy Principles (IPPs) that regulate how Australian and ACT Government agencies may handle personal information, as well as providing individuals with a right to access and, where necessary, correct such information. It also prescribes ten National Privacy Principles (NPPs) which cover parts of the private sector, including all private sector health service providers.
6. These principles are intended to expressly provide for other public interests to be balanced, in certain circumstances, with the public interest in protecting privacy. This is given effect through a serious of prescribed exceptions which apply to the rules established in the various principles.
7. For example, both sets of principles establish the general rule that personal information should generally only be used or disclosed for the purpose for which it was initially collected.[1] However, exceptions to this

[1] IPP 10 regulates the use of personal information by agencies, while IPP 11 regulates disclosures by agencies. In regard to privacy sector organisations, NPP 2 regulates both use and disclosure.

rule include where the use or disclosure may be authorised by law, or where it is reasonably necessary for the enforcement of criminal law.[2]

8. It would appear that these exceptions in the Privacy Act would often provide sufficient scope to permit the appropriate sharing of personal information required to give effect to measures proposed in the Draft Report.

Application of privacy law to national security, law enforcement and other regulators

9. In general, Australian Government law enforcement agencies and agencies with enforcement and regulatory functions such as the Australian Federal Police, the Australian Customs Service, and the Therapeutic Goods Administration are covered by the Privacy Act. Intelligence agencies such as the Australian Security Intelligence Organisation (ASIO) and the Australian Crime Commission (ACC) are exempt from the Privacy Act.

10. State and Northern Territory law enforcement agencies are not covered by the Privacy Act. Some states and the Northern Territory have privacy laws for their public sectors, however operational matters relating to law enforcement are generally not covered by those laws.

Privacy and law enforcement

11. Personal information handling underpins all aspects of law enforcement. Decisions based on poor information or poor information handling can have adverse impacts for individuals, as well as the effectiveness and reputation of law enforcement and national security agencies.

12. For example, privacy principles that require personal information to be accurate and up to date, align comfortably with the needs of law enforcement decision makers.

13. Similarly, the privacy requirement that personal information only be collected where it is relevant for an agency's activities, can help to ensure that decision makers are not encumbered with excessive and unnecessary information.

14. Handling personal information securely and limiting its use for purposes other than that for which it was initially collected not only supports good privacy, but can assist in maintaining the integrity of investigations and inquiries, as well as promoting community trust and confidence in enforcement and regulatory agencies.

15. The importance of maintaining community trust and confidence is underscored by draft recommendation 3(i). This recommendation calls for an informed and vigilant community that is able to assist security and law

[2] These exceptions are variously at IPP 10.1(d), IPP 11.1(e), and NPPs 2.1(f) and (g).

enforcement agencies, including by "…encouraging community members to report suspicious activities to law enforcement authorities".[3]

16. Accordingly, implementing high standards of personal information handling can help maintain information quality and deliver better outcomes for law enforcement and national security agencies and the public. In the Office's view, privacy regulation – in terms of personal information handling – need not be inconsistent with appropriate and necessary law enforcement objectives.

17. At the same time, there may be occasions where the public interest in ensuring the safety and security of the community can be inconsistent with the public interest in promoting privacy. For example, this may occur where law enforcement measures prevent individuals from being able to exercise the opportunity to interact anonymously, or require them to provide personal information that they would not otherwise be obliged to provide.

18. On such occasions, the challenge is to ensure an appropriate balance between these interests, including by seeking to ensure that any diminution in privacy protections are proportionate to, and necessary for, the objective being pursued. This can often be achieved by seeking to ensure that new law enforcement or security measures are accompanied by commensurate protections, such as clearly defined purposes, oversight mechanisms, and statutory limits on the operation and effect of the measures (such as limits on how personal information may be handled).

Draft Recommendation 8: Sharing Information

19. Draft Recommendation 8 on 'Sharing Information' states that COAG agree that all jurisdictions:

> i. review existing chemicals legislation to ensure there is no legal impediment to the appropriate sharing of relevant data between regulators and other nominated government agencies for the purposes of national security, and
>
> ii. establish appropriate arrangements to share information between security and law enforcement agencies, government policy and regulatory agencies, industry and the community in relation to the terrorist misuse of chemicals.

20. While the Office notes that COAG agree that all jurisdictions 'review existing chemicals legislation to ensure there is no legal impediment to the appropriate sharing of relevant data' the Office suggests that the implementation of this recommendation could be recast to focus on the importance of establishing an appropriate legislative framework to authorise and define the scope of the various envisaged measures, rather than on identifying and removing 'legal impediments'.

21. An overarching legislative framework, possibly given effect through the relevant chemicals legislation, which authorise various acts or practices that are necessary for the proposed measures offers the benefits of

[3] Section 7.1 page 23 of the draft Report.

promoting regulatory certainty and the assurance of Parliamentary scrutiny.

22. In addition, such a legislative framework could also ensure that the sharing of information is 'appropriate' (as suggested by the recommendation), by addressing such matters as specifying what acts or practices are permitted and what protections should be afforded to any personal information collected pursuant to them.

23. The Office suggests that an examination of information sharing arrangements between jurisdictions should include consultation with the Privacy Commissioner and equivalent office holders in the states and territories.

24. In addition, for the same reasons as above, the Office suggests amending the sub-heading in Part 8.7 from "Legal Impediments" to "Establishing an appropriate legal framework for sharing personal information"

Providing notice when their personal information is collected

25. The Draft Report discusses possible control measures such as maintaining lists of sellers who have access to restricted chemicals and licensing truck drivers transporting chemicals of concern. Both proposed measures provide examples of where it may be necessary to ensure that there are limits and protections around the handling of personal information. For example, it would seem appropriate that both lists should not be used for purposes unrelated to the security of chemicals of control.

26. If such measures are proposed as part of the framework in the final report, the Office suggests it may be necessary for both private sector organisations and Australian Government agencies to consider appropriate notice requirements under the Privacy Act (NPP1 and IPP2). The Office suggests that an overarching framework for handling personal information would also address this in regard to those entities not covered by the Privacy Act or equivalent state or territory legislation (such as small businesses).[4]

27. The Office would be happy to provide further advice on this matter should such a measure be implemented.

Vetting of individuals in certain circumstances

28. The Office understands that it may be appropriate in some circumstances to collect a certain amount of personal information to screen employees who may have access to chemicals of security concern, and is aware of existing models for vetting current or potential employees in industries such as aviation, maritime security and child care. If such measures were to be considered, they should not be adopted without clear justification and should be proportionate to the object being pursued.

[4] The Privacy Act defines a small business as one with a turnover of $3 million or less.

29. For example, it may not be a proportionate response for individuals to be excluded from employment for offences that have no bearing on their suitability to handle chemicals of concern.

Cross-jurisdictional data sharing in law enforcement contexts

30. The Office notes that the regulation of personal information varies between Australian jurisdictions. While the Commonwealth and some states and territories have privacy regulation, others do not. In some cases, where regulation exists, it can be inconsistent between jurisdictions. This can result in personal information collected in one jurisdiction being afforded different protections, or none, when it is shared with another.

31. Accordingly, the Office suggests that any framework for the sharing of personal information between jurisdictions should be accompanied by detailed consideration of how best to ensure consistent protections as to how it will be handled. Such protections may include not just the rules that apply to its handling, but also appropriate oversight or accountability mechanisms.

32. For example, 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.

33. The Office would welcome the opportunity to be consulted on this matter further.

The "Four A" framework

34. The Office has 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.

Attachment: 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?