



Australian Government

Office of the Privacy Commissioner

Review of Australia's Mutual Assistance Law and Practice

Submission to the Attorney- General's Department

October 2006

Summary

- a) The Office reiterates the broad principles it expressed in its previous submission to the review conducted by the Attorney-General's Department of Australia's extradition arrangements, particularly in regard to the need for clarity and certainty around how individual's personal information may be handled pursuant to mutual assistance matters (see paragraphs 7-9).
- b) This submission also addresses additional matters advanced in regard to mutual assistance arrangements.

Grounds for refusal

- c) The Office suggests that the discretionary grounds for refusal under section 8(2) of the Mutual Assistance Act be expanded to include where the requesting country's arrangements for handling personal information (whether legislative, contractual or otherwise) do not offer privacy protections substantially similar to those applying in Australia (paragraphs 10-14).

DNA from persons without consent

- d) The Office notes the particular sensitivities that many in the community may hold concerning information of this type. DNA information (though not DNA *samples*) will generally fall within the definition of health information under the Privacy Act. This reflects the Parliament's view that it should be afforded additional protections to other, non-health information.
- e) The Office recommends that any proposal for DNA samples, and in turn DNA information, to be collected and disclosed to overseas jurisdictions should be pursued with care. This is particularly the case where the collection is non-consensual and thus the individual's capacity to exercise choice and control is eliminated (paragraph 19-22).
- f) The Office recommends that any non-consensual collection of DNA samples for the purpose of mutual assistance should be subject to a form of judicial oversight similar to that provided in Division 5 of Part 1D, which requires a magistrate to issue an order for the collection (paragraph 27).
- g) The Office recommends that, before disclosing DNA samples or information to a foreign jurisdiction, consideration should be given to the extent to which that jurisdiction offers assurances that any personal information will be handled in a manner that is substantially similar to that which would occur in Australia (paragraph 30).

Providing information from the DNA database

- h) It is the Office's general view that the disclosure of DNA information should, for example, be subject to judicial oversight (paragraph 34).

- i) The Office recommends that it may be appropriate to examine the extent to which enforcement agencies are authorised to disclose DNA information overseas with judicial oversight (paragraphs 35-37).

Telecommunications interception material in the possession of an enforcement agency

- j) The Office suggests that if material obtained under a telecommunications interception warrant is to be disclosed to a requesting country under section 13A of the Mutual Assistance Act, that there should be similar reflection of the offence threshold required to obtain that warrant – such as the requirement that the offence be punishable by a maximum term of imprisonment of 7 years or more (paragraphs 40-42).

Provision of telecommunications interception material and surveillance device material without a domestic investigation

- k) The Office considers that maintenance of appropriate judicial oversight on the collection of information under a telecommunication interception or a surveillance device is essential whether the information is collected in connection with a domestic or an international investigation. As such, it is recommended that this requirement be made more explicit (paragraphs 46-52).

Legislative authorisation for information exchanges

- l) The Office recommends that an authority to exchange information between domestic and overseas agencies be expressly authorised in law (paragraphs 53-55).

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body responsible for promoting an Australian culture that respects privacy. The Privacy Act 1988 (the Privacy Act) covers Australian and ACT Government agencies, businesses with an annual turnover of more than \$3 million, the private health sector, small businesses that trade in personal information and credit providers and credit reporting agencies. The Privacy Commissioner has responsibilities under the Privacy Act and other federal legislation to regulate the way agencies and organisations collect, use, store and disclose individual's personal information.

Background and Discussion Paper

2. The Office welcomes the opportunity to make a submission to the Attorney-General's Department's ('the Department') review of Australia's mutual assistance law and practice (the review).
3. The Minister for Justice and Customs, Senator the Hon Chris Ellison, has released a discussion paper, *A Better Mutual Assistance System: A review of Australia's mutual assistance law and practice – September 2006*. The discussion paper canvasses the need for the reform of mutual assistance arrangements between Australia and other countries and invites comments on a range of issues relating to those arrangements.
4. The terms of reference for the review (at Appendix 1 of the discussion paper) cite domestic and international concerns including the growing importance of combating terrorism and transnational crime and the need for increased cooperation between law enforcement agencies as providing impetus for this review of the *Extradition Act 1988* ('Extradition Act') and the *Mutual Assistance in Criminal Matters Act 1987* ('Mutual Assistance Act').
5. The stated objectives of the review include increasing efficiency and effectiveness of mutual assistance processes and examining the interaction of existing legislation (which would include the Privacy Act) with these processes.
6. Issues that are expressly excluded from the scope of the review include the mutual assistance provisions in the *International Criminal Court Act 2002*, the *International War Crimes Tribunals Act 1995* and police-to-police, or agency-to-agency assistance.

Overview of the Privacy Commissioner's Extradition Submission

7. In March 2006, the Office made a submission to the Department's Review of Extradition Arrangements ('the Extradition Submission').¹ That

¹ Available at http://www.privacy.gov.au/publications/sub_agd_extradition200603.html

submission provides the Office's overarching response to privacy issues arising from transborder law enforcement. Key points made in that submission were:

- On some occasions, the public interest in maintaining the safety and security of the Australian community may warrant diminishing the privacy protections that are otherwise afforded to personal information.
 - The handling of personal information for the purpose of extradition should be transparent and subject to clear rules which ensure that transparency and also provide for accountability.
 - Australian Government agencies should ensure that their handling of personal information, particularly where it is disclosed to overseas jurisdictions, complies with the Privacy Act.
 - There are a number of authorities provided in the Privacy Act under which agencies may disclose personal information. These include for the purpose of enforcing criminal law and where the disclosure is required or authorised by law. However, in regard to the former, this authority should not be interpreted too broadly. In regard to the second exception, the meaning of "law" for the purpose of statutory interpretation may not extend to an international instrument.
 - Agencies may best meet their Privacy Act obligations by pursuing clear legislative authorisations for the handling of personal information pursuant to extraditions. Such authorisations could, most obviously, be achieved by provisions in the Extradition Act and the Mutual Assistance Act which expressly authorise disclosures of personal information for the purposes of those Acts.
 - It would be good privacy practice that personal information should not be transferred to a foreign jurisdiction unless the foreign jurisdiction offers privacy protections substantially similar to Australian privacy standards. Where such protections are not in place, a series of administrative arrangements, memoranda of understanding and protocols may be necessary.
8. The Office has reiterated these comments to the Australian Parliament Joint Standing Committee on Treaties' inquiry into extradition and mutual assistance treaties with Malaysia.²
9. In the Office's view, these comments remain relevant to this current review of mutual assistance arrangements. In both contexts, individuals should feel confident that any personal information handled pursuant to extradition or mutual assistance matters is afforded appropriate privacy protections.

² Available at <http://www.privacy.gov.au/publications/treatsub90806.pdf>.

Response to Issues Raised

Issue 3: Grounds for Refusal

3. Grounds of refusal—general: Are the current grounds of refusal appropriate? Should any of the grounds be removed? Should any of the mandatory grounds be discretionary? Should other grounds be included?

10. The discussion paper considers the grounds on which the Attorney-General may refuse requests for assistance under section 8(2) of the Mutual Assistance Act.
11. An important question for the review is whether the safeguards afforded to personal information under Australian law are also present in foreign jurisdictions to which the personal information may be disclosed. Such a measure is likely to be significant in influencing the degree to which individuals and the community more broadly retain confidence in how personal information is handled in the context of mutual assistance.
12. At present, section 8(2)(e) of the Mutual Assistance Act gives the Attorney-General discretion to refuse a request for assistance where providing the assistance 'would, or would be likely to, prejudice the safety of any person.' While the existing grounds for refusal cover the direct possibility of physical harm resulting from the disclosure, it does not cover other significant adverse consequences that may flow from the mishandling of personal information.
13. Accordingly, the Office suggests that the discretionary grounds for refusal under section 8(2) be expanded. A request could be potentially refused where the requesting country's arrangements for handling personal information (whether legislative, contractual or otherwise) do not offer privacy protections substantially similar to those applying in Australia.

Issue 12: Consent to DNA Collection

12. DNA from persons without consent: Currently, Australia can only obtain DNA material from a person for a foreign country where that person consents to that process. Should Australia allow DNA material to be obtained from a person without the person's consent under mutual assistance in the same way as it can be obtained for a domestic investigation? What safeguards should apply?

14. The Office notes that, in regard to the regulatory scope of the Privacy Act, DNA material (such as bodily samples) falls outside the definition of personal information contained in section 6(1) of the Act. Accordingly, the collection, use and disclosure of DNA samples (as opposed to information obtained from analysing that sample) will not be restricted by the Privacy Act.

15. However, as the Office has previously noted,³ the handling of such information, and the activities leading to its collection, is likely to fall within the broader notion of privacy (which includes bodily privacy) covered by Article 17 of the International Covenant on Civil and Political Rights, a treaty referred to in the preamble to the Privacy Act.
16. The Office also notes that DNA samples are, in general, only of value to the extent that they are capable of being examined and codified into genetic information. A blood sample, by itself, is likely to be of little value to law enforcement. It is the information derived from its analysis and which can be attributed back to an individual, that establishes the sample's utility.
17. The Office has previously argued that the distinctive characteristics of DNA information, including its predictive and familial attributes, and subsequent privacy implications necessitates special protections. In the Office's submissions to the joint inquiry of the Australian Law Reform Commission and Australian Health Ethics Committee into the handling of genetic information ('joint ALRC/AHEC inquiry'),⁴ the Office recommended that genetic information be included within the definition of health information (which is, in turn, a form of "sensitive information") in section 6 of the Privacy Act.
18. In this regard, the Parliament has recently passed the *Privacy Legislation Amendment Act 2006* to ensure that genetic information is afforded the same protections under the Privacy Act as other health information. This measure is consistent with the Office's view, as well as with the findings of the joint ALRC/AHEC inquiry.
19. Accordingly, consistent with the policy intent of the Privacy Act, special care should be afforded to information handling practices that may impact on how genetic information is collected, used or disclosed.
20. An important element of the Privacy Act is that individuals should be able, wherever possible, to exercise an appropriate degree of control over the handling of their personal information. This expectation appears even more reasonable where the information is health information, such as genetic information. This expectation should only be departed from where there is a compelling justification.
21. Particular complexities surrounding consent arise where bodily privacy and the privacy of personal information intersect. The Office notes, for instance, that a tissue sample can be tested multiple times to extract new personal information without necessarily seeking the individual's consent. It may be tested at one time for a DNA match in the context of law enforcement, but at another time to gain predictive health information

³ http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

⁴ The Office's primary and supplementary submissions to the joint ALRC/AHEC inquiry, *Essentially Yours: The Protection of Human Genetic Information in Australia*, are available at <http://www.privacy.gov.au/publications/genesub.pdf> and <http://www.privacy.gov.au/publications/genesub2.pdf> respectively.

about the individual or, in the case of genetic relatives, another individual. In the Office's 2002 supplementary submission to the joint ALRC/AHEC inquiry, the distinction was drawn between DNA testing being used merely to confirm an individual's identity and the examination of DNA samples to "uncover data about a person's genetic makeup".⁵

22. Accordingly, any proposal for DNA samples, and in turn DNA information, to be collected and disclosed to overseas jurisdictions should be pursued with care. This is particularly the case where the collection is non-consensual and thus the individual's capacity to exercise choice and control is eliminated.

Trans-Border Privacy Protections

23. The Office has consistently recommended rigorous privacy protections surrounding the handling of DNA information. The main issues for a system of protections operating across national borders are likely to include authorisation, accountability, complexity and consistency; these matters are discussed in further detail below.

Authorisation

24. Proper systems of authorisation are needed to regulate the circumstances in which non-consensual forensic procedures are conducted. The Office notes the role of Part 1D of the *Crimes Act 1914* in the regulation of such matters for Commonwealth officers. This part sets out the authorisations that apply in regard to collections from suspects and offenders. In turn, different authorisations are prescribed for intimate (including, blood and buccal swab) and non-intimate (including hair and finger prints) collections.
25. In broad terms, non-consensual collections of DNA samples can be authorised by either senior constables (non-intimate collection from suspects or offenders) or magistrates (intimate collections from suspects or offenders).
26. In regard to mutual assistance, it should be recognised that the exercise of these powers is currently premised on the information remaining in Australia and thus subject to other established oversight and accountability mechanisms. It is not apparent that the same degree of assurance would exist with regard to some foreign jurisdictions.
27. Accordingly, the Office recommends that any non-consensual collection of DNA samples for the purpose of mutual assistance should be subject to a form of judicial oversight similar to that provided in Division 5 of Part 1D, which requires a magistrate to issue an order for the collection.

Accountability and oversight

⁵ See paragraph 46.4, available at <http://www.privacy.gov.au/publications/genesub.doc>.

28. It is the Office's general view that the handling of DNA information should be subject to independent accountability mechanisms. As stated in the Office's Extradition Submission (at paragraph 50), community support of law enforcement objectives rests on clear mechanisms of accountability. The Office notes that the Minister has expressed views that are consistent with the Office position.⁶
29. In addition, the *Report of Independent Review of Part 1D of the Crimes Act 1914 - Forensic Procedures*, saw "...effective accountability mechanisms as crucial to maintaining public confidence in the use of DNA analysis for law enforcement purposes."⁷ Such mechanisms may include providing individuals with the ability to make complaints, and audit powers for oversight bodies.
30. Accordingly, a key issue that should be addressed as part of any move to allowing the non-consensual collection and disclosure of DNA samples or information to a foreign jurisdictions is the extent to which this accountability could be provided and by what mechanisms. For example, consideration could be given to the accountability and oversight mechanisms provided in the recipient jurisdiction.

Complexity and Consistency

31. In its submission to the joint ALRC/AHEC inquiry, the Office noted the difficulties that were apparent in achieving uniform national consistency in the handling of DNA information, including in regard to the rules that govern its handling in each jurisdiction.
32. These issues are likely to be compounded in the transnational context. Within Australia, there are mechanisms for driving consistency across jurisdictions, such as the Standing Committee of Attorneys-General, as well as common legal and institutional structures and systems. Such mechanisms would seem less likely to be available regarding the exchange of DNA information for the purpose of mutual assistance. This again highlights the need for consideration to be given to the need for administrative arrangements, memoranda of understanding and protocols with recipient jurisdictions.
33. This approach is consistent with, for example, National Privacy Principle 9 (applying to private sector organisations). This principles reflects a policy

⁶ On March 2, 2001, Minister Ellison addressed Parliament in relation to the CrimTrac DNA database:

"It is therefore very important that we take steps to ensure that there is adequate independent oversight of compliance with agreed procedures. In view of the inter-jurisdictional nature of the scheme it is vital that we have arrangements that ensure that the oversight function is like the system itself: interconnected and properly coordinated. These arrangements must also ensure that complaints can be investigated easily without jurisdictional barriers becoming a problem."

⁷ See, 'Executive Summary' available at [http://www.ag.gov.au/agd/WWW/rwpattach.nsf/viewasattachmentpersonal/\(CFD7369FCAE9B8F32F341DBE097801FF\)~2Executive+Summary.pdf/\\$file/2Executive+Summary.pdf](http://www.ag.gov.au/agd/WWW/rwpattach.nsf/viewasattachmentpersonal/(CFD7369FCAE9B8F32F341DBE097801FF)~2Executive+Summary.pdf/$file/2Executive+Summary.pdf).

setting that organisations should, when sending personal information overseas, take reasonable steps to ensure that the privacy protections afforded to that information will be substantially similar to that which applies in Australia. An organisation may do this by having a reasonable belief that the recipient is subject to law, binding scheme or contract which effectively provides similar protections.

Issues 13 and 14: Providing Information from the DNA Database and DNA Matching

13. Providing information from the DNA database: Currently, Australia can provide DNA information stored on the National Criminal Investigation DNA Database (NCIDD) to foreign countries by using the take evidence or production order proceedings in the Mutual Assistance Act or executing a mutual assistance search warrant for specifically identified DNA. DNA information can also be provided where it is in the possession of an enforcement agency. Are the current mechanisms for providing this DNA information appropriate? Are there better mechanisms for doing this?

34. The Office has noted above the particular privacy sensitivities associated with DNA information (see, paragraphs 14-22). In addition, in considering this issue, the Office refers to the comments provided above concerning the need for appropriate authorisation, oversight and accountability (24-30). It is the Office's view that the disclosure of DNA information should, for example, be subject to judicial oversight.

35. The Office notes the three mechanisms in the Mutual Assistance Act which can be used to disclose DNA information to a foreign country, only two of which require any form of judicial oversight or process. The third mechanism (disclosure where material has been lawfully obtained by an enforcement agency⁸) may undermine the assurances offered by the two other available mechanisms.

36. Accordingly, given the Office's comments above concerning authorisation and oversight, it may be appropriate to examine the extent to which enforcement agencies are authorised to disclose DNA information overseas.

37. In this regard, the Office does not necessarily advocate the complete elimination of this mechanism. For example, it may be appropriate to consider the extent to which such exchanges are or could be regulated by other mechanisms, either legislative or administrative.

14. DNA matching: Currently, Australia cannot 'match' a DNA sample from a foreign country against the NCIDD unless the mutual assistance search warrant criteria are met. Should Australia allow controlled access to the NCIDD under mutual assistance for the purpose of DNA matching?

⁸ The example of the Australian Federal Police is provided.

38. Given the sensitivity of genetic information, and the noting the importance of appropriate authorisation mechanisms, the Office would, in absence of compelling justification for the contrary, generally recommend that the handling of DNA samples, including its matching, should be subject to judicial oversight. Such oversight is currently afforded by Division 2 of the Mutual Assistance Act.

Issue 15: Providing Telecommunications Interception Material already in the Possession of an Enforcement Agency

15. Telecommunications interception material already in the possession of an enforcement agency: Currently, Australia can only provide telecommunications material through take evidence or production order proceedings under section 13 of the Mutual Assistance Act. Should Australia be able to provide telecommunications interception material and other telecommunications data such as stored communications, under section 13A of the Mutual Assistance Act in the same way that Australia can currently provide surveillance device material under this section?

39. The discussion paper states that telecommunications interception material already in the possession of an enforcement agency (after being lawfully obtained) cannot be provided to a foreign country. The paper states that the Mutual Assistance Act could be amended to allow for telecommunications material to be disclosed in this circumstance (the proposal).

40. The Office considers that the requirement that telecommunication interception material must be lawfully obtained is a key element to maintaining appropriate protections for individuals against unwarranted telecommunication interception. In order for information to be lawfully obtained in Australia, the Office understands that it must be collected subject to the restrictions in the *Telecommunications (Interception and Access) Act 1979* (TIA Act), with the stipulated requirements to obtain a warrant. Such warrants may only be issued in regard to “serious offences”, defined in section 5D of the TIA to include, amongst other things, murder, kidnapping, child pornography and other offences carrying a penalty of 7 or more years imprisonment.

41. Preserving the requirements under which the information may be collected by telecommunications interception ensures that appropriate judicial oversight over the use of telecommunications interception warrants is maintained.

42. Section 13A(2) of the Mutual Assistance Act describes the circumstances under which material obtained through the use of a surveillance device can be provided to a requesting country. Those requirements include that the offence is punishable by a maximum term of imprisonment of 3 years or more. The Office notes that this mirrors the requirements for the issue of a surveillance device warrant. The Office suggests that if material obtained

under a telecommunications interception warrant is to be disclosed to a requesting country under section 13A of the Mutual Assistance Act, then the offence threshold for the purpose of section 13A should be similar to that which is required to obtain the warrant – such as the requirement that the offence be punishable by a maximum term of imprisonment of 7 years or more.

43. The Office notes the privacy objects of the TIA Act⁹ include that communications that are not necessary for a particular investigation at hand should be destroyed as soon as practicable. In relation to stored communications, this object has been given statutory effect through the new provision enacted in 2006 in section 150(1) of the TIA Act which requires the destruction, “forthwith,” of information or a record that was obtained by accessing a stored communications, where the chief officer of the relevant agency “is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2)”.
44. This proposal should not derogate from this principle. There may be a risk that telecommunications interception material collected incidentally, or that is no longer necessary for an investigation, by an Australian enforcement agency is “warehoused” or kept indefinitely on the basis that it may be of use to a foreign country at some future time. As such, the proposal could be incompatible with good privacy practice and the privacy objects of the TIA Act.
45. As some countries do not have privacy laws similar to Australia, there should be a mechanism in the legislation to ensure that the relevant foreign country gives an undertaking not to use or disclose the interception material for secondary purposes beyond the matter for which it is initially collected.

Issue 16: Provision of telecommunications interception material and surveillance device material without a domestic investigation

16. Interception of telecommunications and use of surveillance devices without a domestic investigation: Currently, Australia cannot intercept telecommunications, access stored communications, or use most surveillance devices solely at the request of a foreign country. Where resources are available, should Australia be able to intercept telecommunications and use surveillance devices at the request of a foreign country without the need for a domestic investigation?

46. The paper states that currently Australia cannot intercept telecommunications, access stored communications, or use most surveillance devices solely at the request of a foreign country. The proposal is that Australia intercept telecommunications and use

⁹ As articulated in the *Telecommunications (Interception) Act 1979 Annual Report to 30 June 2004* at 2.2.

surveillance devices of individuals at the request of a foreign country without the need for a domestic investigation (the proposal).

47. The Office would support a requirement that the proposal only apply in relation to relatively serious offences. The Office notes that cultural, historical and legal issues in the foreign country may criminalise conduct that would not be the case in Australia, or, if criminalised in Australia, would not be considered as a serious offence.
48. In the Office's extradition submission (paragraphs 37-39),¹⁰ the Office noted that permitting information flows to foreign countries for the purposes of enforcing foreign laws that criminalise conduct that is lawful in Australia would create an inconsistency in Australian privacy regulation, allowing personal information flows offshore that are not permitted onshore.
49. There needs to be recognition that the serious offence should have an equivalent in Australian law, or that the penalty is comparable to that which would be imposed under Australian law, before any disclosure to the foreign country occurs.
50. The collection of information through intercepted communications, surveillance devices or stored communications should be on the basis of appropriate oversight and review mechanisms, for example, by the issue of a warrant from a judicial officer. The statement "*Obtaining telecommunications interception and surveillance device material in Australia for a foreign investigation could occur in exactly the same way as for a domestic investigation*" appears to imply that it would be necessary for a warrant to be obtained under Australian legislation in order to proceed with the collection of information.
51. The Office considers that maintenance of appropriate judicial oversight on the collection of information under a telecommunication interception or a surveillance device is essential whether the information is collected in connection with a domestic or an international investigation. As such, it is recommended that this requirement be made more explicit.
52. As some countries do not have privacy laws similar to Australia, there should be a mechanism in the legislation to ensure that the relevant foreign country gives an undertaking not to use or disclose the interception material for secondary purposes before the interception material is disclosed.

¹⁰ Available at

http://www.privacy.gov.au/publications/sub_agd_extradition200603.html#mozTocId183262.

Issue 25: Legislative Authorisation for Information Exchanges

25 Privacy: Mutual assistance can involve personal information flows between a range of agencies in Australia and between Australia and foreign countries for law enforcement purposes. Should the Mutual Assistance Act expressly identify and authorise the personal information flows in the mutual assistance process?

53. The discussion paper also considers whether the Mutual Assistance Act should expressly identify and authorise the personal information flows in the mutual assistance process (at paragraph 6.4.3).
54. The Office welcomes this proposal, which is consistent with recommendations made in the Office's extradition submission (at paragraphs 26-36).
55. In particular, the Office welcomes the discussion paper's statement that the amending provisions be specific, and would not authorise information sharing generally.

Improving domestic capacity

56. The Office's Extradition Submission noted the potential value of administrative measures to foster compliance with the Privacy Act. Such measures could include guidance material to APS officers on the appropriate application of the Privacy Act to mutual assistance matters. The Office reiterates the potential value of such material in clarifying the role of the Privacy Act and notes that a function of this type may fit comfortably as a project similar to those described in section 7.1.1 of the discussion paper ('Enhancing skills and knowledge').
57. The Extradition Submission also suggested that the information flows in extradition be "mapped" to identify where the various collections, uses and disclosures are likely to occur. Similarly, such a process may be useful to specifically identifying those points in the information lifecycle where the Privacy Act is most likely to be relevant. It appears that a mapping exercise of this type could progress the objectives outlined in section 7.1.3 on "Clarifying roles and responsibilities".