

KD  
328.9404  
AGR  
LEG

**“In Confidence”: The House of Representatives Standing Committee  
on Legal and Constitutional Affairs Report of its inquiry into the  
protection of confidential personal and commercial information held  
by the Commonwealth**

**Government Response**

20 Aug 2002

## “In Confidence”: The House of Representatives Standing Committee on Legal and Constitutional Affairs Report of its inquiry into the protection of confidential personal and commercial information held by the Commonwealth

The Report deals with a range of issues affecting a number of portfolios. The Report has been taken into account in the formulation of policies that have been announced and implemented since the Report was prepared. As a result, the Government considers many of the recommendations of the Report have now been superseded.

The Government considers that a higher level of awareness and increased culture of privacy has developed in the Australian Public Service since the time the Report was prepared. Given developments in electronic communication, transmission and availability of information in recent years, many agencies have increased their focus on privacy issues. Most Commonwealth agencies' web sites contain privacy policy statements.

The Government notes that the Committee has used a variety of terms to describe the categories of information to which their recommendations apply (eg, third party information, confidential third party information, confidential information, etc). Unless otherwise stated, the response to each recommendation applies to both personal and commercial third party information whether confidential or not, and proposes a response accordingly. However, as the *Privacy Act 1988* only applies to personal information, whether confidential or not, the recommendations dealing with that Act are taken only to apply to personal information.

The Government response to the Committee's recommendations is as set out below:

### **Administrative safeguards and the accountability of senior managers**

#### **Recommendation 1**

**The Committee recommends that there be a description of responsibilities of heads of agencies in the *Public Service Act 1922*. The description should include responsibility for the protection of confidential third party information held by the Commonwealth Government.**

Not accepted. The *Public Service Act 1999* sets out the responsibilities of heads of agencies and of other public service employees without unnecessary prescription. Under that Act, heads of agencies are bound by a Code of Conduct which requires, among other things, Australian Public Service (APS) employees comply with all applicable Australian laws and not to make improper use of inside information. Further, the Public Service Regulations provide that an APS employee must not, except in the course of his or her duties as an APS employee or with the agency head's express authority, give or disclose, directly or indirectly, to any person any information about public business or anything of which the employee has official knowledge.

### **Recommendation 2**

**The Committee further recommends that the head of an agency be responsible for providing all agency staff with comprehensive guidelines and operating manuals relating to the protection of confidential third party information that it holds. In addition, the head of an agency should be responsible for ensuring that all staff of the agency receive training in the protection of confidential third party information and compliance with relevant guidelines and operating manuals.**

Accepted in principle. This responsibility is now encompassed in the revised Protective Security Manual. The revised Manual was endorsed by the Government on 14 September 2000 and made available to agencies in December 2000.

Further, all agencies are responsible for complying with obligations under the *Privacy Act 1988*.

### **Recommendation 3**

**The Committee recommends that for each agency that collects third party information, the agency head be responsible for monitoring the on-going need for that information. Each agency should report annually to the Privacy Commissioner on the outcome of that monitoring with regard to personal information. Each agency should state in its annual report the outcome of that monitoring with regard to commercial information.**

Not accepted. The accountability arrangements under the *Privacy Act 1988* already make sufficient provision for the audit of privacy protection in agencies. The Government considers these arrangements are effective and should remain in place rather than instituting a new reporting mechanism that may have significant resource implications.

### **Recommendation 4**

**The Committee recommends that the power to disclose confidential third party information held by a Commonwealth Government agency be given only to a limited number of clearly identified senior executive officers who are, where practicable, at a level no lower than SES Band 2.**

Not accepted. Implementation of this recommendation would be impractical for the effective delivery of government administration. The issue is adequately addressed by mechanisms under the *Freedom of Information Act 1982* and the *Privacy Act 1988*.

### **Recommendation 5**

**The Committee recommends that agencies be required to provide, within 14 days of the disclosure, reasons to the Privacy Commissioner for an authorised disclosure of personal information being made.**

Not accepted. Such a requirement is impractical and would impose unreasonable costs on some agencies and on the Office of the Federal Privacy Commissioner which would be difficult to absorb. Normal file records will exist which are subject to review as part of the Privacy Commissioner's audit function.

### **Recommendation 6**

**The Committee recommends that each Commonwealth Government agency keep a record of authorised disclosures of confidential third party information for the purpose of checking the legitimacy of access to such information. The record should include the names of individuals and organisations about whom information is disclosed, the names of individuals and organisations to whom that disclosure is made, and the date of disclosure.**

Accepted in principle. Consistent with proper file management practices, file records of such disclosures will exist. In relation to personal information, file records of disclosures are subject to review as part of the Privacy Commissioner's audit function. Further, in relation to disclosures of personal information for law enforcement or revenue protection purposes, there is a requirement in Information Privacy Principle (IPP) 11.2 of the *Privacy Act 1988* to include in the record of personal information a note of the disclosure.

### **Implications of ICAC findings for Commonwealth agencies**

#### **Recommendation 7**

**The Committee recommends that each agency have a senior manager who is responsible for implementing and promoting privacy standards and the protection of information within an agency. The chosen senior manager should be a clearly identified senior executive service officer who is, where practicable, at a level no lower than SES Band 2.**

Not accepted. Other initiatives which have promoted awareness of privacy in Commonwealth agencies over the last 10 years make implementation of this recommendation unnecessary. The Government believes that the Privacy Contact Officers network, established by the Privacy Commissioner, appropriately fulfils the goals of this recommendation. In addition, all APS employees must comply with the APS Code of Conduct which includes a requirement to comply with all applicable Australian laws and not to make improper use of inside information. Breaches of the Code may attract strong penalties including reduction in salary and termination.

#### **Recommendation 8**

**The Committee recommends that each agency head establish an Information Protection Committee with the objective of monitoring the protection of third party information within the agency and disseminating information which would foster the protection of that information.**

Not accepted. Other initiatives which have promoted awareness of privacy in Commonwealth agencies over the last 10 years make implementation of this recommendation unnecessary. The Government believes that the Privacy Contact Officers network, established by the Privacy Commissioner, appropriately fulfils these functions.

#### **Recommendation 9**

**The Committee recommends that the senior executive service officers of agencies inform themselves of the demand for confidential third party information held by their respective agencies.**

Not accepted. Other initiatives which have promoted awareness of privacy in Commonwealth agencies over the last 10 years make implementation of this recommendation unnecessary.

The Government considers that an increased level of awareness of, and support for, privacy principles can best be achieved through the Office of the Federal Privacy Commissioner's efforts to encourage the development of a culture that respects privacy within both the public and the private sectors.

#### **Recommendation 10**

**The Committee recommends that agencies be required to enter into inter-agency agreements on the disclosure of confidential personal information to be approved by the Privacy Commissioner.**

Qualified acceptance. As in any other area of Government regulation, agencies are responsible for ensuring compliance of their own operations with the *Privacy Act 1988*. The Information Privacy Principles (IPPs) set out in the *Privacy Act 1988* govern disclosure of personal information between agencies. Any inter-agency agreements on the disclosure of personal information must be consistent with the IPP obligations. Where appropriate, agencies are encouraged by the Attorney-General's Department to enter into memoranda of understanding covering communications between them relating to personal information. However, specific statutory provisions applicable to particular agencies sometimes make such agreements inappropriate.

#### **Recommendation 11**

**The Committee recommends that all agencies adopt a comprehensive security system such as that provided by the Protective Security Manual. Agencies should adapt the general standards to their particular circumstances.**

Accepted. The revised Protective Security Manual was prepared by the Attorney-General's Department, approved by the Government, and made available to agencies in December 2000. It is the principal means for disseminating Commonwealth protective security policies, principles, standards and procedures to be followed by all Commonwealth agencies for the protection of official information and resources.

To assist government departments and agencies in adapting these standards to their particular circumstances, the Protective Security Coordination Centre of the Attorney-General's Department, and the Defence Signals Directorate provide appropriate training.

#### **Recommendation 12**

**The Committee recommends that all agencies adopt adequate standards for computer security. Guidelines should be developed after incorporating advice from existing government agencies with expertise in computer security.**

Accepted in principle. Security issues for computer systems are being addressed at a number of levels. Agency specific security improvements have been made since the Report was released and the general problem of protecting against hacker attacks, viruses and other intrusions are being addressed as part of the Government's e-security policy and initiatives to protect the National Information Infrastructure.

### **Recommendation 13**

**The Committee recommends that the Australian National Audit Office conduct security efficiency audits of computer systems.**

Noted. Performance audits are carried out at the discretion of the Auditor-General, reflecting his statutory independence from the Government and Parliament. Protective security audits on computer security have been conducted in the past. The ANAO will consider conducting performance audits of computer systems in the future within the context of the annual audit work program, which is endorsed by the Joint Committee of Public Accounts and Audit (JCPAA).

### **Recommendation 14**

**The Committee recommends that sufficient resources be allocated to the Australian National Audit Office to support this role.**

Noted. Should the Auditor-General decide to undertake a wider program of dedicated audits of the type recommended, it would normally be part of the annual audit work program, which would be funded through the normal budgetary process. Should any additional funding be required, the Auditor-General would bring the matter to the attention of the JCPAA.

### **Recommendation 15**

**The Committee recommends that security manuals specifically address the process required to authorise work taken out of the fixed office site and the security features of portable computers.**

Accepted. This issue is specifically addressed in the revised Protective Security Manual. In particular, Part C of the manual covers Information Security when dealing with electronic media (including portable computers), and Part H provides Security Guidelines on Home-based Work.

### **Recommendation 16**

**The Committee recommends that the *Privacy Act 1988* be amended to make a contractor to a Commonwealth agency primarily liable for observance of the Information Privacy Principles as if the contractor were the agency.**

Accepted. This recommendation has been implemented by the *Privacy Amendment (Private Sector) Act 2000* which commenced on 21 December 2001. Under the amended Privacy Act, agencies are required to take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice that would breach an Information Privacy Principle if it were done or engaged in by the agency. The Privacy Commissioner has been given jurisdiction to directly investigate the actions of a contracted service provider and to make determinations as appropriate.

## Legal safeguards and the legitimate transfer of information

### Recommendation 17

**The Committee recommends that transfers of confidential personal information between Commonwealth Government agencies should be regulated by the *Privacy Act 1988*, rather than by the secrecy provisions in specific statutes. The Privacy Act should be reviewed and amended to ensure that the necessary degree of protection for transferred information is maintained.**

Not accepted. Certain secrecy provisions such as those found in the *Customs Act 1901* and the *Australian Security Intelligence Organisation Act 1979* need to be maintained either to protect interests other than the interest of the individual to whom the personal information relates (such as the security of Australia), or to penalise corrupt dealing in personal information or the soliciting of that information. It would be difficult to address the specific security concerns surrounding secrecy provisions within the common framework of the *Privacy Act 1988*.

However, for general protection of personal information, the Government considers that the *Privacy Act 1988* is adequate to ensure protection of any personal information transferred between Commonwealth agencies. The disclosure of any personal information held by a Commonwealth agency is governed by Information Privacy Principle 11. IPP 11.3 requires the person, body or agency to whom personal information is disclosed under IPP 11.1, only to use that information for the purposes for which it was given. Receiving agencies are also governed by the IPPs.

### Recommendation 18

**The Committee further recommends that each Commonwealth Government agency keep a record of authorised transfers of confidential personal information between agencies for the purpose of checking the legitimacy of access to such information. The record should include the names of individuals and organisations about whom information is transferred, the names of individuals and organisations to whom that transfer is made, and the date of the transfer.**

Accepted in principle. Consistent with good file management practices, file records of disclosures of personal information are subject to review as part of the Privacy Commissioner's audit functions. Where disclosures of personal information are made for law enforcement or revenue protection purposes, the *Privacy Act 1988* requires inclusion of a note of any such disclosure in the record of personal information.

### Recommendation 19

**The Committee recommends that the *Privacy Act 1988* be amended to provide that where an Act other than the Privacy Act deals expressly with a matter of permissible use and disclosure, IPPs 10 and 11 do not operate to provide additional grounds for disclosure.**

Not accepted. The *Privacy Act 1988* provides a general level of privacy protection for personal information held by agencies. Information Privacy Principles 10 and 11 prohibit use and disclosure of personal information except in certain circumstances. The exceptions listed in IPPs 10 and 11 do not compel use or disclosure where a particular use or disclosure falls within the exceptions listed. Agency specific legislation may place tighter restrictions on the

protection afforded to particular personal information held by particular agencies. In that case, the restrictions in the specific legislation would override the general base standards in the Privacy Act. Therefore, amendment of the *Privacy Act 1988* is not necessary, as Information Privacy Principles 10 and 11 do not provide additional grounds for use and disclosure.

**Recommendation 20**

**The Committee recommends that as part of the review of the scope of the *Privacy Act 1988*, the exceptions in the Information Privacy Principles 10 and 11 be more specific.**

Not accepted. Experience in the application of the Information Privacy Principles has confirmed the necessity for them to be stated in terms that are sufficiently flexible and therefore capable of applying in a variety of circumstances.

**Recommendation 21**

**The Committee recommends that the *Privacy Act 1988* be amended to clarify the meaning of the term 'protection of the public revenue'.**

Not accepted. This issue is adequately dealt with by Guideline 41 of the *Plain English Guidelines to Information Privacy Principles 8-11* issued by the Office of the Federal Privacy Commissioner.

**Recommendation 22**

**The Committee recommends that permitted transfers of confidential third party information between Commonwealth Government agencies be accommodated by way of exceptions to the Information Privacy Principles.**

Not accepted. Desirable transfer of personal information that would otherwise be in breach of the IPPs can be accommodated by legislative amendment to the relevant agency legislation. The Government considers it preferable that specific legislative amendment be made to deal with the unique features of the information handling obligations of particular agencies. The aim of the *Privacy Act 1988* is to set out general principles of universal application.

**Recommendation 23**

**The Committee recommends that uniform controls for data-matching carried out by Commonwealth Government agencies be made a legal obligation and incorporated into the *Privacy Act 1988*.**

Not accepted. The Office of the Federal Privacy Commissioner has issued Data-Matching Program (Assistance and Tax) Guidelines under the *Data-matching Program (Assistance and Tax) Act 1990* compliance with which is mandatory. Other data-matching in Commonwealth administration is covered by Guidelines issued by the Office of the Federal Privacy Commissioner in February 1998. These guidelines were developed and reviewed in consultation with Commonwealth agencies to assist in ensuring that data-matching programs are designed and conducted in accordance with sound privacy practices.



#### **Recommendation 24**

**The Committee further recommends that major data-matching programs proceed with the authority of a clearly identified senior executive service officer who is, where practicable, at a level no lower than SES Band 2.**

Not accepted. The Office of the Federal Privacy Commissioner will keep the effect of major data-matching programs under review in accordance with his functions under section 27 of the *Privacy Act 1988*.

#### **Recommendation 25**

**The Committee recommends that agency heads be provided with a discretion to permit disclosure of confidential personal information held by the agency where notification of or consent for disclosure is not a reasonable possibility. This discretion is to be subject to:**

- **the necessity of the disclosure;**
- **the disclosure being an integral part of the use for which the information was obtained; and**
- **notification or consent procedures being demonstrably inappropriate.**

Accepted in principle. The *Public Service Act 1999* and the *Privacy Act 1988* already provide mechanisms addressing the concerns to which this recommendation is aimed.

Disclosure of personal information is subject to Information Privacy Principle 11 in the *Privacy Act 1988*. IPP 11 provides that the disclosure of personal information to a person, body or agency may be made if:

- the person the information is about has been told, or is otherwise likely to know, that the information is usually disclosed to that person, body or agency; or
- the person the information is about has consented; or
- the disclosure is necessary to protect against a serious and imminent threat to a person's life or health; or
- the disclosure is reasonably necessary to enforce the criminal law or a law imposing a pecuniary penalty, or to protect public revenue.

In relation to agency heads, section 76 of the *Public Service Act 1999* provides that regulations may authorise the disclosure, in specific circumstances, of personal information. Regulation 9.2 of the Public Service Regulations provides that an agency head may disclose personal information (within the meaning of the *Privacy Act 1988*) that is in the possession, or under the control, of the agency head where the disclosure is necessary for the performance of an outsourced personnel function.

#### **Recommendation 26**

**The Committee further recommends that agencies be required to report, within 14 days of the disclosure, all such exercises of that discretion to the Privacy Commissioner.**

Not accepted. Such a requirement is impracticable and would impose unnecessary costs on both the agency and the Office of the Federal Privacy Commissioner. However, records of

disclosure should be maintained for review as part of normal file keeping measures and would be available to the Privacy Commissioner in carrying out his audit functions.

**Recommendation 27**

**The Committee recommends that agency heads be provided with a discretion to permit disclosure of confidential personal information where a disclosure is clearly in the individual's interest and consent could not be obtained.**

Accepted in principle. Provision for the disclosure of this information can be made by regulation under section 76 of the *Public Service Act 1999*. Also, Information Privacy Principle 11 allows for the disclosure of personal information if the disclosure is necessary to protect against a serious and imminent threat to a person's life or health.

**Recommendation 28**

**The Committee further recommends that agencies be required to report, within 14 days of the disclosure, all such exercises of that discretion to the Privacy Commissioner.**

Not accepted. Such a requirement is impracticable and would impose unnecessary costs on both the agency and the Office of the Federal Privacy Commissioner. However, records of disclosure should be maintained for review as part of normal file keeping measures and would be available to the Privacy Commissioner in carrying out his audit functions.

**Application and rationalisation of the criminal law**

**Recommendation 29**

**The Committee recommends that the protection of confidential personal and commercial information should be the subject of general offence provisions located in the *Crimes Act 1914*.**

Accepted in principle. The Committee's recommendation will be taken into account in reviewing unnecessary secrecy provisions as part of the Government's progressive development of the Criminal Code.

The Government recognises that the criminal law has a role to play in the protection of third party information. However, it is important not to overstate the significance of the criminal law, nor to neglect the role which alternative measures may play in setting appropriate standards and procedures for handling information.

**Recommendation 30**

**The Committee recommends that general offence provisions, protecting confidential third party information held by the Commonwealth Government and its agencies, be included in the *Crimes Act 1914*. The Committee further recommends that the information protected by these general provisions be defined by reference to other enactments.**

Accepted in principle. Subject to some qualifications as in the Government response to recommendation 29.

### **Recommendation 31**

**The Committee recommends that unauthorised dealing in confidential third party information held by the Commonwealth Government and its agencies, should be prohibited at every point on the distribution chain by general offence provisions in the *Crimes Act 1914*.**

Accepted in principle. The general provisions presently cover the unauthorised disclosure of information by public officers for profit or otherwise.

The penalties for unauthorised disclosure by public officers for profit will be considered in reviewing unnecessary secrecy provisions as part of the Government's progressive development of the Criminal Code.

### **Remedies and the need for compensation**

#### **Recommendation 32**

**The Committee recommends that the *Privacy Act 1988* be amended so that, if there is an unauthorised disclosure of personal information held by a Commonwealth agency, a person's right to compensation from the Commonwealth agency would be established by the unauthorised disclosure, regardless of whether there has been a breach of an Information Privacy Principle by the agency.**

Not accepted. While the objective of ensuring the protection of individuals' privacy is endorsed, the responsibilities of agencies for the action of their employees in relation to privacy are already broad. The Office of the Federal Privacy Commissioner is the appropriate regulatory body for handling complaints and alleged breaches of the *Privacy Act 1988*.

### **Access to third party information**

#### **Recommendation 33**

**The Committee recommends that consideration be given to amending the *Archives Act 1983* by replacing references to 'information relating to the personal affairs of any person' with 'personal information about any person' and inserting the definition of 'personal information' found in the *Freedom of Information Act 1982* and the *Privacy Act 1988*.**

Accepted in principle. In July 1998 the Australian Law Reform Commission (ALRC) published a report entitled *Australia's Federal Record*, reviewing the *Archives Act 1983*. The issue of changing terminology in the *Archives Act 1983* to include a 'personal information' definition consistent with other legislation is being considered in the development of a Government response to the ALRC report.

#### **Recommendation 34**

**The Committee recommends that the Privacy Commissioner coordinate a review of the reasons for allowing access to public registers, particularly where technology permits the information contained on public registers to be used for purposes in addition to that for which it was collected. The review should also consider whether any limits need to be imposed on access to public register information or on the purposes for which such information can be used.**

Accepted in principle. This issue is particularly relevant given developments in technology that allow for easy access and use. The Attorney-General's Department is currently considering the issue of use of personal information contained in public registers. The Department will liaise closely with the Office of the Federal Privacy Commissioner in examining this issue.

#### **Recommendation 35**

**The Committee recommends that the *Commonwealth Electoral Act 1918* be amended so that the end use restrictions which currently apply to electoral roll data contained on tape or disk also apply to the same data contained on microfiche or in hard copy.**

Accepted in principle. This issue is currently under consideration by the Australian Electoral Commission as part of its review of the access provisions contained in the *Commonwealth Electoral Act 1918*.

#### **Recommendation 36**

**The Committee recommends that the Australian Health Ministers Advisory Committee and the Australian Association of Cancer Registries jointly explore options and implement measures which will ensure patients are notified, verbally and in writing, that identifiable data concerning their condition may be forwarded to cancer registries, the Australian Institute of Health and Welfare and may be released to external researchers.**

Accepted in principle. This issue has been addressed by the *Privacy Amendment (Private Sector) Act 2000*. National Privacy Principle 1.3 requires organisations that collect personal information to take reasonable steps to inform the individual at the time of collection (or as soon as practicable after collection) of a number of matters, including the organisations (or types of organisations) to which the organisation usually discloses information of that kind. Organisations that provide personal information to cancer registries or the Australian Institute of Health and Welfare (either under statute or by agreement) will therefore be obligated to inform individuals of that fact.

This issue is also being considered as part of the Government's development of a privacy framework in relation to the development of a national electronic health record network.

### **Recommendation 37**

**The Committee further recommends that public education programs be conducted to inform the public that certain confidential personal information may be forwarded to registries and the Australian Institute of Health and Welfare, and released to external researchers.**

Qualified acceptance. The issue of public education and awareness has been addressed in part by the *Privacy Amendment (Private Sector) Act 2000*. The Office of the Federal Privacy Commissioner has developed guidelines on how health information is protected under the Act.

### **The need for a national privacy code**

#### **Recommendation 38**

**The Committee recommends that the protections provided by the Information Privacy Principles should be extended to all confidential third party information by way of a national privacy code.**

Accepted in principle. This recommendation has been addressed in part by the enactment of the *Privacy Amendment (Private Sector) Act 2000* which extends privacy protection to personal information held by private sector organisations. The Act implements National Privacy Principles that apply to personal information held by private sector organisations. It also includes provision for the development of industry specific privacy codes. These codes must provide at least an equivalent level of protection for individual personal information to that of the National Privacy Principles. The National Privacy Principles are similar in content to the Information Privacy Principles.

#### **Recommendation 39**

**The Committee recommends that the proposal for a national privacy code be placed on the agenda, for the earliest possible meeting of the Council of Australian Governments.**

Not accepted. The issue of a national code has been addressed by the enactment of the *Privacy Amendment (Private Sector) Act 2000* which applies to private sector organisations.

