Joint Committee of Public Accounts and Audit

Management and Integrity of Electronic Information in the Commonwealth

SUBMISSION

Malcolm Crompton
Federal Privacy Commissioner

January 2003

Table of Contents

1 Executive Summary

1.1 Introduction

Ensuring data integrity and the efficient and effective management of electronic information by governments are important objectives in the pursuit of broader public goals, including the promotion of an Australian culture that respects privacy, attaining a secure environment for all Australians and the delivery of optimal government services.

While privacy and other public policy goals might generate competing interests, this does not have to result in the trade-off of one priority for another. It is possible to have a secure society, an efficient economy and an effective public service system that embraces and respects the privacy of citizens. Only as a last resort, should it be necessary for parliaments and public sector agencies to act in ways that meet critical social objectives, while also reducing privacy protection for individuals.

This inquiry, by the Joint Committee on Public Accounts and Audit, into the integrity and management of electronic information held by the Commonwealth, is most welcome. This is a timely opportunity to take stock of current information-handling practices, to identify new issues, developments and trends that affect how the Commonwealth handles individuals' personal information, and to consider where improvements in regulation or guidance may be warranted. This submission aims to assist in each of these areas.

The submission begins with an overview of key themes, followed by recommendations to the Committee. The body of the submission is structured in three parts: a review of privacy in the Commonwealth and the experience of the Office of the Federal Privacy Commissioner (the Office) in its regulation of the *Privacy Act 1988* (Cwth) to date; a consideration of emerging issues, developments and trends that affect (or will affect) Commonwealth data-handling; and some comments on the adequacy of the current legislative and guidance framework. The submission is followed by attachments aimed at assisting the Committee in its consideration of the current privacy framework and related issues.

1.2 Key issues

Australians expect that the personal information they provide to Commonwealth agencies will be held in trust. Agencies have many duties to the Australian community, including privacy obligations that arise from the Privacy Act and other statutes.

The integrity, security and good management of personal information are significant aspects of protecting individual privacy, particularly in electronic and on-line environments. The privacy of personal information, however, is a broader concept, of which security and data integrity are a part. Other aspects of privacy include limits on the collection of information, its use and disclosure, and giving people access to information about them that is held by agencies. Together these elements give rise to obligations aimed at promoting respect for the dignity of individuals and ensuring that they retain reasonable control over their personal information.

Strategies for data management, maintaining data integrity or data security often involve the collection of more information about individuals than is already held by the agency, the re-use of personal information, the increased cross-checking of data, or increased levels of individual identification. All such strategies can intrude on other aspects of privacy. A balanced privacy approach does not call for a halt in such strategies. Rather, better privacy outcomes are likely to be achieved if the full privacy impact of new proposals, initiatives or systems is considered at an early stage (see section 3.1.5.1). Such assessments can facilitate the building of good privacy (and its elements, including data integrity and security) into the very fabric of the initiative, so that its implementation readily delivers effective data management.

This submission reflects on how agencies have been managing privacy, and especially data integrity and security, to date. It draws on the experience of the Office through complaint-handling, investigations, and audits. The submission also draws on the Office's experience in providing comment and advice on new initiatives at the policy and legislative development stage, as well as in relation to operational issues.

Through the Office's complaint-handling (see section 3.1.1), for example, it has become apparent that in the electronic handling of personal information, the damage to an individual that can flow from a privacy breach has the potential to be magnified compared with breaches arising from manual systems. Moreover, complaints about data security, accuracy and the improper disclosure of data make up a significant proportion of all complaints received. Hence, while complaints relating specifically to the electronic handling of information are relatively low at this stage, with the increase in on-line data management and in its complexity, the potential for harm to individuals' privacy is an issue that cannot be underestimated.

Through audits of agencies (see section 3.1.2), the Office has found that in some cases agencies either do not have adequate information technology (IT) security policies, or that such policies are not consistently administered. A simple, but significant issue, for instance, is the security of portable IT devices, such as laptop computers. In some cases, agencies may need to more carefully consider the design and testing of their website

security measures. In relation to the development of data management systems, problems arising from mass mail-outs, either paper or electronic, remain an area of particular privacy risk.

On occasions when the management of personal information by government agencies has been unsatisfactory, it continues to attract a high level of media interest (see section 3.1.4). In turn, such media interest has the potential to reduce the community's confidence in government agencies and the services they provide. Since 2000, the Office has issued 23 media statements over incidents involving the public sector handling of personal information. Media attention has focused particularly on events involving electronic records of personal information held by government agencies. Issues that have captured the attention of the media include, the Australian Taxation Office's (ATO) disclosure of personal data relating to the Australian Business Number (ABN) from its website, and a Child Support Agency (CSA) email sent to a group of clients, which also divulged the email addresses of other members of the group (involving approximately 400 email addresses).

In the policy and systems development context (see section 3.1.5), the Office has observed that agencies tend to consult on privacy issues in the later stages of policy and legislative design or at the point of the implementation of strategies – often, at this stage in the process, it is difficult to alter and improve approaches. Sometimes, privacy is perceived as an 'add-on', to be considered only at the operational level. Also, privacy can be perceived merely as an impediment to the agency's primary objective, thus needing to be traded off to achieve that objective.

The Office continues to advocate, as it always has, for the need for agencies to systematically consider, at an early stage, the privacy implications of their new activities, so that privacy becomes part of the development of their business case and related decision-making processes. Unfortunately, after fourteen years, this approach is still not established in Commonwealth public service management. Hence Recommendation 1 (see section 3.1.5.1) that agencies be required to undertake privacy impact assessments for new initiatives, proposals and systems. Such assessments, involving the use of a balanced framework for identifying privacy issues, has been proposed by the Office when considering areas as diverse as anti-terrorism initiatives, the use of public key infrastructure, and developments in law enforcement.

Having played a significant part in the privacy regulatory frameworks of jurisdictions in Canada, Hong Kong and New Zealand, these assessments are now compulsory in some Canadian jurisdictions. Furthermore, the USA's *E-Government Act of 2002* requires privacy impact assessments for certain data collection activities of its Federal government.

Significant new issues and trends are emerging in electronic information management, either as a response to technological opportunity or to external forces driving the search for new solutions, and where the impact on the privacy protection of Australians is (or may be) significant. Changes in our environment, including the greater emphasis on national security following the terrorist attacks in the USA and Bali in 2001 and 2002, or

the increasing levels and awareness of identity theft and fraud, act as imperatives to shape public policy in relation to the collection and management of information about the citizenry.

With the move towards greater on-line provision of government services, there is demand for better methods of identification and authentication. This is increased by whole-of-government approaches to service provision.

These changes and developments can affect individuals' privacy either directly or as a result of strategies developed in response to them. Also, there can be a tendency to look toward old solutions that are often outmoded and ineffective in delivering the desired policy aims, such as the single identifying number or the identity card. Debates on these options happened in Australia over fifteen years ago, and continue to be challenged around the world today. The objection is not against the legitimate identification and authentication of an individual, but in relation to how this is done so that it minimises privacy intrusion and limitations on autonomy, while ensuring that the necessary checking of identity can occur effectively.

Just as technology can drive new opportunities for efficiency in data management, so its potential can surely be harnessed to deliver smart, new identification/authentication mechanisms. This leads to Recommendation 3 (see section 3.2.6.1) that there be a coordinated, cross-Commonwealth approach to this issue, with projected savings (arising from improved identification and authentication) being invested in the development of a privacy enhancing means of delivering on this need.

The on-going challenge for agencies remains to respond to their legislative and policy obligations, and the changing environment, in ways that do not reduce individuals' privacy. Some agencies have learned and developed their skills and approaches in this area, just as the Office has increased its knowledge and experience. The opportunities for the future lie in harnessing technological developments to enhance privacy through its incorporation into the 'weave' of each new project or initiative that involves the handling of personal information, most particularly where that information is handled electronically.

2 Recommendations

The Privacy Commissioner makes the following recommendations:

Recommendation 1 – that those Commonwealth agencies with significant personal information handling responsibilities be required to report to the Privacy Commissioner, annually, regarding the number (and nature in trends of) privacy complaints that they handle.

These agencies would include, amongst others, Centrelink, the Australian Tax Office, Department of Family and Community Services, the Child Support Agency, the Department of Health and Ageing, the Health Insurance Commission, the Department of Veterans' Affairs, the Department of Immigration, Multicultural and Indigenous Affairs and Comcare (see section 3.1.1).

Recommendation 2 – that Commonwealth agencies be required to undertake privacy impact assessments at the beginning of the development of new proposals and initiatives involving the handling of the personal information of the Australian community.

These assessments should be published unless national security or law enforcement considerations outweigh the public interest in the publication. If an assessment is not to be published, it should be copied to the Privacy Commissioner, the Attorney-General's Department; the Department of Finance and Administration and the Department of Prime Minister and Cabinet (see section 3.1.5.1).

Recommendation 3 – that the Cabinet Handbook and the Department of Prime Minister and Cabinet's Drafter's Guide be amended to more specifically guide agencies in their early assessment of the privacy impact of new proposals relevant to Cabinet Submissions, Cabinet Memoranda and like documents (see section 3.1.5.1).

Recommendation 4 – that the Committee endorse the approach announced by the newly established Information Management Strategy Committee (IMSC) to lead a coordinated, cross-Commonwealth initiative on electronic identification/authentication and proof of identity issues. The Committee should give consideration to recommending that the Privacy Commissioner be co-opted as a member of the IMSC to ensure the necessary consideration of privacy.

The IMSC should be well resourced in order to properly consider privacy, including by investing projected savings (both savings arising from the reduced incidence of fraudulent identity and its implications for government, as well as the efficiencies generated through the reduction in duplicated services) into the building of a privacy-enhancing identification/authentication mechanism or approach.

The IMSC can take a key role in resolving one of the major inhibitors to the development of new identification/authentication models in both the public and private sectors, by leading work toward an agreed set of standards that will set the benchmark for the necessary privacy (including security) requirements of all new initiatives in this area (see section 3.2.6.1).

Recommendation 5 – that agencies be expected to continue to have a Privacy Contact Officer (PCO), including a commitment by each agency to the importance of the role, with the necessary seniority and level of resources available to underpin the effective operation of the role (see section 3.3.1).

Recommendation 6 – that the gap in guidance between the Information Privacy Principles (in the Privacy Act), the Defence Signals Directorate (DSD) and the Commonwealth Protective Security Manual (PSM) be filled by more practical, operational guidance. For example, an on-line authentication guide developed by an agency such as the National Office on the Information Economy (NOIE) in association with the Office (see section 3.3.3).

Recommendation 7 – that the Office be resourced to discharge the additional functions arising from the implementation of these recommendations (see section 3.3.3).

(Note: there is a section reference after each recommendation to assist the reader in locating the recommendation within the body of the submission).

3 The privacy, confidentiality and integrity of the Commonwealth's electronic data, including its management and security by Commonwealth agencies

3.1 Privacy in the Commonwealth: learning from the current regulatory framework

Data integrity can be an important issue in achieving a range of ends, some of which are particularly relevant in the electronic data environment. These include: information privacy objectives such as keeping personal information secure; organisational or policy objectives; national security objectives; reducing the cost and maximising the efficiency of providing government services by reducing fraud or wastage; or providing those services in different ways, which increasingly involves using electronic means.

The Information Privacy Principles (IPPs) in the Privacy Act set the minimum legal framework by which most agencies must approach data integrity, security and management; whether in relation to service delivery to customers or clients, or in designing policy and systems to meet agency objectives.

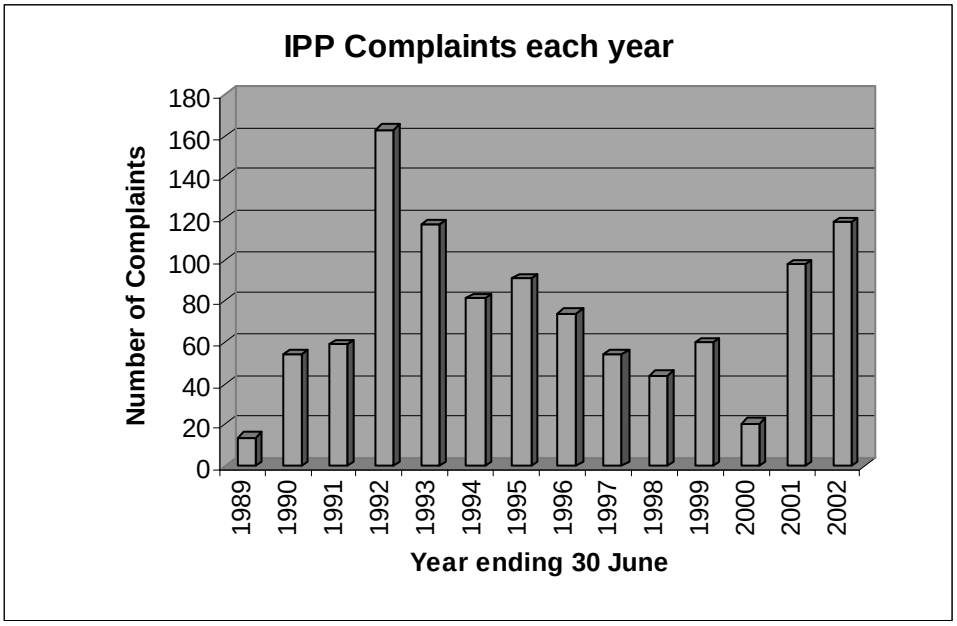
Based on data available from the Office's complaints records and its limited audit program, in respect of agencies' responsibilities to keep personal information accurate, up-to-date and secure, the 'scorecard' is quite good. The Office's experience over many years suggests that agencies do well in managing sensitive information, while there is reasonable compliance with the Privacy Act in the management of less sensitive personal information. There are, however, areas for improvement.

Generally, agencies do less well in thinking about privacy during the development and implementation of policy, legislation and systems. The tendency has been to consider privacy as something that arises only at the implementation stage, or else to think of it as a value that must be traded off against other interests.

Increasingly there is recognition, in Australia, of privacy's role in setting up the environment of trust and confidence that is necessary if individuals are to take up options involving on-line mechanisms for receiving services or providing information. This recognition, however, does not always translate into early consideration of privacy issues in the development of on-line systems. There is a challenge, then, in moving beyond a reactive, compliance-based approach, to develop new initiatives in ways that incorporate privacy from the outset, so that they inherently protect personal information by virtue of their design.

3.1.1 Overview of privacy complaints regarding agencies

The Office investigates a range of complaints made by individuals about agencies each year. The Office will generally only commence an investigation if a person has first tried to resolve the issue directly with the agency concerned. Agencies, such as Centrelink, have explicit procedures in place to try and handle as many complaints as possible as internal matters, so that the individual does not need to go the Privacy Commissioner. The Office does not have figures on the numbers of complaints that agencies deal with directly. It is anticipated, however, that the number of complaints investigated by the Office reflects a small percentage of the overall number of privacy complaints made by individuals.



Complaints received in 2001-02

Total complaints received in 2001/2002 (all jurisdictions, including the new private sector jurisdiction)	632
Total complaints against Commonwealth agencies (under the IPPs)	118
Total IPP complaints under those IPPs most relevant to the inquiry (namely, IPPs 4, 8 and 11)	95
Number of complaints that relate to electronic handling of personal information	15

The Office's experience in relation to complaints, data integrity and electronically managed personal information suggests that:

- Electronic handling of personal information can magnify the damage that flows from a privacy breach;

- Complaints about security, data accuracy and the improper disclosure of information constitute a significant proportion of the total number of complaints, and so point to areas vulnerable to privacy risk; and

- Complaints specifically with an explicit electronic information management focus are relatively low at this point.

Recommendation 1:

That those Commonwealth agencies with significant personal information handling responsibilities be required to report to the Privacy Commissioner, annually, regarding the number (and nature in trends of) privacy complaints that they handle.

These agencies would include, amongst others, Centrelink, the Australian Tax Office, Department of Family and Community Services, the Child Support Agency, the Department of Health and Ageing, the Health Insurance Commission, the Department of Veterans' Affairs, the Department of Immigration, Multicultural and Indigenous Affairs and Comcare.

3.1.2 Overview of privacy audits of agencies

Agencies have responsibilities to audit their own data management processes. In this regard, the Office has observed a trend toward agencies seeking external privacy audit advice to enhance their processes.

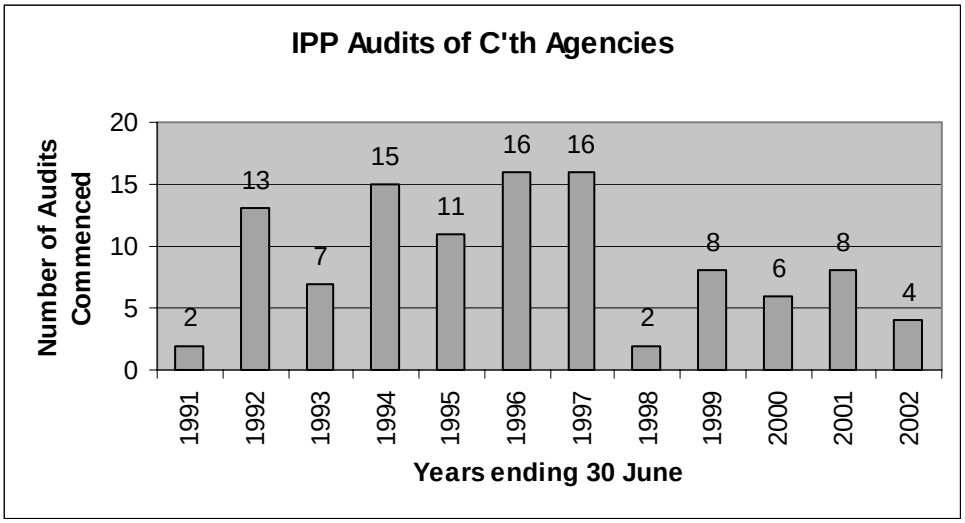
Agencies' own monitoring activities are bolstered by the audits conducted by the Office, as well as by other agencies, such as the Australian National Audit Office (ANAO).

The Privacy Commissioner's audit function is an important and effective tool in promoting compliance with the Privacy Act, developing agencies' understanding of privacy risks and raising awareness of their privacy obligations. Audits can also help to promote confidence within the community that systems relating to personal information (held and managed by the Commonwealth) are scrutinised and reviewed, helping to ensure that the information, ultimately, is used and protected appropriately.

The audit process, however, is resource intensive. Annually, the Office can audit only a small sample of agencies and their activities. Hence, audits need to be well targeted. The Office uses a risk management strategy to ensure its audits focus on activities with high privacy risk. When determining whether to undertake an audit, the Office takes into account a range of issues, such as:

Risk factors	
1	The agency, organisation or program has recently come into existence
2	New legislation is being administered by an agency
3	The sensitivity of the personal information held by the agency
4	The quantity of personal information held by the agency
5	The number of complaints received against the agency
6	Any media coverage of issues of privacy concern
7	New technology is being implemented by the agency
8	New procedures are being adopted by the agency
9	How long it is since the previous audit, and whether there are any outstanding issues
10	Whether there has been a risk reported to the Office from other sources

The following graph sets out the annual number of IPP audits conducted during the period between 1991 and 2002.



Note:

The first decrease in the number of audits (for 1998) followed significant budget cuts to the Human Rights and Equal Opportunity Commission (HREOC), of which the Office was then a part.

Furthermore, in 2001-02 the Office had to reallocate its resources from audit activities to other priority areas, most notably in meeting peak demand for advice regarding the introduction of the new legislation applying to the private sector from December 2001. The Office intends to return its focus to audit activities in the medium term, should resources be available.

3.1.3 Privacy audit findings and privacy risks

The Office's view, from available evidence arising from audits, and with some exceptions (discussed below), is that generally agencies have a reasonable record in managing the privacy and security of personal information.

There are some common audit findings, however, where issues have been identified that indicate more work needs to be done to manage privacy risks and improve practice. In relation to electronic information the common findings include:

- Agencies either do not have adequate IT security policies or such policies are not consistently administered;
- Mass mail outs are an area of particular privacy risk;
- There is a need for greater attention to the security of portable IT devices, such as laptop computers and personal digital assistants (eg. Palm Pilots);
- Agencies may need to more carefully design and test website security measures;
- Agencies need to do more to ensure that their websites display adequate privacy policies, as well as adequate advice to users about security risks.[1] Where the agency collects personal information though its site, it needs to ensure there is an adequate IPP 2 (collection) notice; and
- Information technology (IT) outsourcing contracts do not always contain appropriate privacy clauses – and in some cases contracts are not sufficiently monitored.

The ANAO's audits have given rise to similar findings. For example, some recent findings regarding the Department of Health and Ageing (DHA) include that:

> Because of the nature of the data collected, held and processed within Health's IT systems, the confidentiality and privacy of information are important business issues. Although designated responsibility for privacy matters, at the commencement of this audit the Information Planning and Privacy Committee (IPPC) had not developed policy or guidelines to ensure compliance with the information privacy principles of the Privacy Act. Since that time, the IPPC has allocated a task to a subcommittee to address privacy issues with a completion date of June 2002 (38).

[1] *Privacy Compliance Audit: Commonwealth Government Websites 2001*, Office of the Federal Privacy Commissioner, available at http://www.privacy.gov.au/publications/wsr01.html

> The ANAO's review of application security plans indicates that information privacy requirements have not been adequately addressed as none of the plans reviewed had considered privacy issues (39). [2]

An audit of the Department of Veterans' Affairs (DVA) outsourcing practices found that:

> … However, DVA had not reviewed the contractor's processes; and it did not monitor data movements on the IT infrastructure, which would have provided assurance that controls and systems were operating effectively (paragraph 3.32). [3]

3.1.3.1 Common logical security findings in audits

When conducting an audit into the information handling practices of a Commonwealth agency, the auditors examine the IT security arrangements in place to protect personal information held in the agency's databases. This involves looking at the measures in place to protect the information against loss, unauthorised access, use, modification or disclosure, and against other misuse (as specified by IPP 4).

The Office expects that agencies will have appropriate measures in place to secure personal information against external security risks and inappropriate internal access. This includes physical measures (such as, adequate perimeter security for buildings and internal physical access restrictions to the IT system hardware), as well as logical security measures (such as, user identification (userID) and password protection, backed up with audit trials for access to records).

A common finding in audits of Commonwealth agencies is that either adequate IT security policies are not in place, or they are not consistently administered.

A common scenario that should be prevented by such a policy involves an employee or contractor who previously had legitimate access to personal information held in the agency records, and then ceases to work for the agency, but there is no procedure in place to ensure that the individual can no longer gain access to the information (or such a procedure is not followed). In these cases, the information is at risk if the individual can log into the system remotely or if they physically enter the premises and use a network terminal.

Another scenario involves different levels of access to information being set for different staff, yet without a strong culture of internal security. For example, an agency's IT system may permit a staff member to use the same password continuously, or for an unacceptably long period. This often leads to other staff (who should not have access to certain information) finding out the staff member's password in ways that may seem harmless – someone may be asked to carry out a one-off task for the principal staff member and be told their password so they can do so. Then the principal staff member

---

[2] *Information Technology at the Department of Health and Ageing*, ANAO, 2002, available at http://www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256BF8002282B7

[3] *Management of an IT Outsourcing Contract: Department of Veterans' Affairs*, ANAO, 2002, available at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256BAB0078C8F1

doesn't follow up and change their password. Or, staff can become complacent about the security of their password and record it somewhere that other staff can easily see it or find it.

3.1.4 Breaches, or potential breaches, of the Privacy Act that have attracted media attention

Management of personal information by government agencies can attract a high degree of media interest. Since 2000, the Office has issued 23 media statements over the handling of personal information by public sector agencies. Media attention has focussed particularly on events involving electronic records. Major issues have included:

- Australia Post's Australian Family Lifestyle Survey;
- Australian Electoral Commission – the use of the electoral roll to assist in a proposed mail out of GST information;
- Australian Taxation Office – disclosure of ABN data and personal information from its website, particularly involving small businesses operating from a residential address;
- Child Support Agency – an email sent to clients that also divulged 400 other email addresses;
- Family and Community Services and 'The Source' website – a government website that collected personal information and then provided it to another organisation, following which the individuals involved received unsolicited marketing material;
- Government agencies and the loss or theft of laptops; and
- Treasury – the GST Assist website was hacked with registered suppliers' bank account details rendered insecure.

3.1.4.1 Case studies – questionable management of electronic personal information

- **GST Assist website**

The GST-Assist website was developed to provide an electronic web-based supplier registration system as part of the introduction of the GST. The website collected businesses', as well as some individuals' bank account numbers and other information. An individual managed to access this personal information and circulated it (though only to those named in the record), thus highlighting considerable potential for misuse of the information.

The Office investigated the incident and confirmed that the absence of appropriate security measures in the Treasury Department's GST-Assist website, prior to 29 June

2000, was a breach of the Privacy Act. The GST Start-Up Assistance Office took prompt action to improve security by placing the information behind the Department of Treasury's website firewall. The security testing that had been carried out on the GST-Assist website had been limited and primarily concerned with business access requirements. It did not adequately address the need to protect personal information in the database from unauthorised access.

- **The Source website**

During April 2002, the Department of Family and Community Services (FACS) ran thirty-four online 'Win Free Stuff' competitions that attracted thousands of entries. This occurred through a website that FACS manages and calls 'The Source'. In June 2002, the Website Editor of The Source agreed to send marketing emails to the 'Win Free Stuff' entrants on behalf of students of RMIT University (Melbourne), who were running a research project to send spiders into space with NASA.

Staff responsible for The Source website acted quickly and took appropriate action when it became obvious that they had made unauthorised use of their website visitors' email addresses. The Office conducted an investigation into the matter and found that FACS had breached IPP 10.1 (which states, in summary, that a record-keeper with possession or control of a record that contains personal information and that was obtained for a particular purpose shall not use the information for any other purpose unless one of a number of specified exceptions apply – in this case, none of the exceptions applied).

At the time of the breach, the Website Editor of The Source was new to the role and had not attended a privacy awareness training session; they had also not checked their actions with staff in the Administrative Law Unit regarding the Commissioner's *Guidelines for Federal and ACT Government Websites*.

The breaches have now been adequately addressed by FACS and measures are now in place to prevent similar breaches occurring, including:

- Completing a privacy audit of FACS' websites;
- Changing FACS' website privacy statements to make them clearer;
- Destroying the database that held the website visitors' details;
- Clearing up links so visitors can be sure which site they are supplying information to;
- Conducting privacy awareness training for all staff and ensuring that the training will be repeated regularly; and
- Appointing the Privacy Contact Officer to the Change Management Committee.

3.1.5 Privacy in policy and systems developments

The Privacy Commissioner's privacy advice role – set out at sections 27.1 (b), (e) and (f) of the Privacy Act – involves examining proposed legislation, preparing guidelines and commenting on new policy proposals, as well as on implementation activities in areas

where there are privacy implications. This role gives the Office a useful insight into the privacy and security of the Commonwealth's electronically held personal information.

The Cabinet Handbook and the related 'Drafter's Guide' (issued by the Department of Prime Minister and Cabinet) give recognition to this role, noting that 'specialist agencies should be consulted on any submission or memorandum proposing matters directly relevant to their specialist functions …. [including] the Privacy Commissioner (privacy implications, including with respect to legislative proposals).'[4]

During the fourteen years that the Privacy Act has been in place there have been significant changes in how the Commonwealth provides services and manages personal information, including:

- Greater emphasis on fraud management and compliance with a related increase in the use of verification and data-matching activities between agencies;

- Changes in government administration, particularly in separating policy and service provider functions, and in moving toward a 'one-stop shop' approach for many services;

- Technological changes and a move to greater on-line government;

- Greater emphasis on national security and boarder control issues; and

- Moves towards an electronic health environment that operates across federal, state and non-government sectors.

In the midst of these emerging issues and trends, agencies have approached privacy in different ways. Some agencies have taken steps to build a culture of privacy and ensure that they have access to privacy expertise. This might include appointing Privacy Contact Officers (PCOs), establishing specialist privacy teams, or consulting legal firms, privacy consultants or privacy advocates.

The Office's experience, however, has been that agencies tend to consult on privacy in the later stages of policy and legislative development, or in the implementation stages, when it is difficult to change already developed approaches. There can be a perception that privacy, and obligations arising from the Privacy Act, are 'add-ons' that only need be considered at the operational level, or alternately that privacy is an impediment to other objectives and can be traded off to achieve these objectives.

The Office has been advocating for some time that agencies should be obliged to systematically consider the privacy implications of their new activities as part of the development of their business case and related decision-making processes. This approach is not yet well established in public service management.

---

[4] Available on the website of the Department of Prime Minister & Cabinet at http://www.dpmc.gov.au/docs/displaycontents1.cfm?&ID=101

3.1.5.1 Privacy impact assessments

Taking careful, early and systematic account of privacy in decision-making processes is likely to improve privacy outcomes and the overall outcomes of a new project. This can be achieved through using a privacy impact assessment (PIA).

A PIA is a balanced assessment of any actual, or potential, effects that an activity or proposal may have on individuals' privacy, and then looking at ways in which any adverse effects can be mitigated.

To date, the Office has canvassed the benefits of balanced privacy assessment frameworks in three main contexts:

- The Privacy Commissioner's submission to the Senate Legal and Constitutional Legislation Committee's 2002 Inquiry into the Terrorism Bills (see section 3.2.1);

- In a speech to the Australian Institute of Criminology's Conference, 'New Crimes or New Responses: Future Directions, Crime Prevention, Legal Responses and Policy' in June 2001. Here, a framework similar to that set out in the above submission was advanced and several case studies examined; [5]

- The Privacy Commissioner's *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals.* [6] The Privacy Commissioner developed these guidelines in consultation with the National Office for the Information Economy (NOIE) after it identified the need. The guidelines advise agencies to undertake a privacy impact assessment before implementing a new public key infrastructure (PKI) system, or before significantly revising or extending an existing PKI system.

PIAs have played a significant part in the privacy regulatory framework of jurisdictions as diverse as Canada, Hong Kong and New Zealand. They are now compulsory in some Canadian jurisdictions. A recent paper prepared by Blair Stewart (New Zealand Deputy Privacy Commissioner) gives a good overview of the PIA approach, and provides examples of situations where they have been used.[7]

Most recently, the US *E-Government Act of 2002* requires privacy impact assessments for certain data collection activities of US Federal government agencies.

---

[5] *Preserving Privacy in a Rapidly Changing Environment*, Privacy Commissioner's speech to the Australian Institute of Criminology Conference, Canberra, April 2001, available at http://www.privacy.gov.au/news/speeches/sp34note.doc

[6] Available at http://www.privacy.gov.au/government/guidelines/index.html#a

[7] *Privacy Impact Assessment: Some Approaches, Issues And Examples* Blair Stewart, Assistant Commissioner, Office of the Privacy Commissioner, New Zealand, available on a more general page about PIAs at http://www.privacy.org.nz/sintprf.html

Drawn from the Office's experience in this area, the Privacy Commissioner makes the following recommendations:

Recommendation 2:

That Commonwealth agencies be required to undertake privacy impact assessments at the beginning of the development of new proposals and initiatives involving the handling of the personal information of the Australian community.

These assessments should be published unless national security or law enforcement considerations outweigh the public interest in the publication. If an assessment is not to be published, it should be copied to the Privacy Commissioner, the Attorney-General's Department; the Department of Finance and Administration and the Department of Prime Minister and Cabinet.

Recommendation 3:

That the Cabinet Handbook and the Department of Prime Minister and Cabinet's Drafter's Guide be amended to more specifically guide agencies in their early assessment of the privacy impact of new proposals relevant to Cabinet Submissions, Cabinet Memoranda and like documents.

3.1.6 Cross agency data-matching

Data-matching involves bringing together data from different sources – whether within, or from outside, the Commonwealth public sector - and comparing it. Much of the data-matching done by agencies, where it is subject to the Privacy Act, aims to identify people for further action or investigation. For example, records from different agencies are compared to identify people who are being paid benefits to which they may not be entitled, or to identify people who are not paying the right amount of tax.

Data-matching is a powerful administrative and law enforcement tool. It allows information from a variety of sources to be brought together, compiled and applied to a range of public policy purposes at a vastly lower cost than manual methods. For instance:

- In benefit-paying programs, it can be used to check the information clients provide and identify those clients who are receiving an incorrect level of benefit;

- In revenue collection, it can allow the identification of undeclared income and so help in the efficient allocation of audit resources;

- In criminal investigation, it can provide vital intelligence, showing up otherwise invisible links between persons and investigations;

- Data-matching can also play an important role in reducing fraud relating to the Commonwealth. For many types of fraud, it is one of the few instruments available for determining that an offence has been committed.

These are important purposes and data-matching can make a valuable, and sometimes pivotal, contribution. On the other hand, data-matching can have significant privacy implications:

- It may involve the use of data for purposes other than those for which it was originally supplied or obtained. Moreover, those purposes may be outside the reasonable expectations of the people the information is about. A basic privacy principle is that, generally, personal information should be used only for the purpose for which it was obtained. So, people should know how and why their personal information is being collected and how it will be used. Departures from this principle need to be strongly justified on public interest grounds;

- Data-matching can involve the automatic examination of the personal information of many thousands of people about whom there are no known grounds for suspicion and in relation to whom no action is warranted. This may be done without the knowledge of the people whose information is being scrutinised;

- Data-matching relies on agencies gaining access to large amounts of information, some of which may be personal information, from a range of sources. Agencies may be inclined to keep unmatched information for possible future use, even though it has no immediate application; and

- Data-matching is far from perfectly reliable. A data-matching program may fail to distinguish between individuals with similar personal details; input data may be faulty; errors may be made in programming; or difficulties may be caused if similar fields in different databases are not precisely comparable.

The ATO and assistance agencies must comply with the *Data-matching Program (Assistance and Tax) Act 1990* (the Data-matching Act) and related guidelines issued by the Privacy Commissioner under the Act, when conducting data-matching using tax file numbers.

In 1992 the Commissioner issued advisory guidelines called *The use of data matching in Commonwealth administration – Guidelines*. These were later revised in 1995 and 1998. These guidelines are for voluntary adoption by agencies when conducting matching that is not specifically regulated by the Data-matching Act. Most agencies with any involvement in data-matching have agreed to abide by them.

Both the Data-matching Act and the Commissioner's voluntary guidelines seek to address privacy concerns by ensuring that, wherever possible:

- The estimated costs and benefits of data-matching programs are taken into account before commencement;

- Information about the data-matching programs in which Commonwealth agencies participate is made publicly available;

- People whose data is used in data-matching programs are informed about those uses;

- The output of data-matching programs is not accorded undue weight and is checked before action is taken, where this could be detrimental to the individual concerned;

- Data obtained for use in a data-matching program is not retained once it has served the specific purposes of that program; and

- the effectiveness of data-matching programs is carefully examined.

Both the Data-matching Act and the Commissioner's guidelines, however, apply only to comparisons of large datasets. With today's more sophisticated IT options, it is increasingly easy to link databases to allow the matching of information on a record-by-record basis rather than in large batches.

New proposals involve matching and cross-checking are now more likely to occur in 'real time' (as the person applies for a benefit or service, or undertakes a transaction), rather than by way of retrospective, batch-style data-matching.

So, while the Data-matching Act provides a good framework for regulating some data-matching, given the continued growth in data-matching proposals and the progression in the manner in which matching occurs, it is increasingly likely that forms of cross-matching will not be regulated by the Data-matching Act or covered by the Commissioner's voluntary guidelines. Existing frameworks of law and guidance may, therefore, need review and amendment in the near future.

3.1.7 *Commonwealth Services Delivery Agency Act 1997*

The *Commonwealth Services Delivery Agency Act 1997* provided for the establishment of Centrelink – and a framework for this agency to provide services (in the manner of a 'one-stop shop') on behalf of other agencies. This represented a significant shift in the way the Government collected, maintained and used information about people as Centrelink initially drew together data previously held by at least three different agencies. Centrelink has since expanded, now providing services on behalf of over fourteen agencies.

From a privacy perspective, the key issues were: the interaction between clients and agency staff, and the extent to which individuals could control whether information about their dealings with agencies under other government programs might be used for a current, but unrelated transaction; the information flows between Centrelink and its 'client' agencies; the respective agency responsibilities for record holding and information management (integrity, security etc.); and limits on the use and disclosure of information.

These matters were subject to extensive consultation between the Office and the agencies concerned, resulting in privacy guidelines on some matters. The consultations, however, took place toward the end of the development process with little opportunity to consider

alternative models, or to find ways to assess the overall impact of the proposed changes on people's privacy in dealing with government.

While determining the overall privacy impact of the Centrelink changes now is probably unachievable, research conducted by the Office (and published in July 2001), shows that generally Australians regard government agencies as reasonably trustworthy (with a mean score of 3.4 out of 5).[8] On the other hand, 14 per cent of respondents said they had decided not to deal with a government agency due to privacy concerns.[9] Though these figures do not directly reflect attitudes to the Government's centralised approach to service delivery, they do show that there is room for improvement in dealing with privacy issues, with the potential that poor handling of privacy issues will damage trust and diminish service uptake.

3.1.8 Project Gatekeeper

Project Gatekeeper was launched in May 1998. NOIE oversees Gatekeeper, which is part of the Government's E-commerce and on-line strategy. Gatekeeper provides a framework for the use of public key technology (PKT) in Commonwealth agencies as a response to security and identification issues for on-line transactions.[10]

Early in the process, privacy issues were identified as likely to be important. Privacy strategies have been built into the supplier accreditation process that Gatekeeper established. NOIE also recognised that different privacy issues emerge where agencies want individuals to use PKT. As mentioned, NOIE invited the Privacy Commissioner to develop privacy guidelines to assist in this area.[11] The guidelines were issued in December 2001.

3.1.9 Compliance with the *Guidelines for ACT and Federal Government World Wide Websites*

The Internet has become an important means, and an increasing opportunity, for the delivery of government services and information. Good website privacy practice is important to ensure that Commonwealth agencies handling personal information through their websites do not interfere with the privacy of individuals.

To assist agencies in adopting best privacy practice, and in complying with the Privacy Act, the Privacy Commissioner issued *Guidelines for Federal and ACT Government World Wide Websites* in May 1999. The guidelines provide specific guidance for Commonwealth agencies in the application of the IPPs to their websites. The guidelines

---

[8] *Community attitudes towards privacy in Australia,* Office of the Federal Privacy Commissioner, 2001 http://privacy.gov.au/publications/rcommunity.html#4.5

[9] *Community attitudes towards privacy in Australia,* Office of the Federal Privacy Commissioner, 2001 http://privacy.gov.au/publications/rcommunity.html#4.3

[10] More information available at http://www.NOIE.gov.au/projects/confidence/Securing/Gatekeeper.htm

[11] *Privacy and Public Key Infrastructure: Guidelines for agencies using PKI to communicate or transact with individuals*, Office of the Federal Privacy Commissioner, 2001, available at http://www.privacy.gov.au/government/guidelines/index.html#a

cover four aspects of personal information handling: openness, collection, security and publication. In April 2000, the Government included the guidelines in its Government Online strategy, requiring agencies to comply by 1 June 2000.

In 1999, the Office conducted a preliminary survey of Commonwealth websites to assess compliance with the guidelines. A further and more formal audit was conducted with the results presented to agencies in November 2000. In August 2001, the Office published the results of a follow-up audit to assess progress with compliance.[12] While levels of compliance with the guidelines have improved since the 2000, it is clear that a good deal remains to be done:

- While the proportion of Commonwealth websites that display privacy statements has increased from 18 per cent in 1999 to 69 per cent in 2001, it is a matter for concern that nearly a third of Commonwealth agency websites still did not display a privacy statement;

- Less than half (45.4 per cent) of all websites that collect personal information had adequate IPP 2 statements,[13] or a direct link to a privacy statement; and

- Less than half (42 per cent) of all the websites audited warned users of the risks of transmitting data across the Internet. All websites that collect personal information should provide a warning of the risks associated with using the Internet in this way, or provide secure facilities for transferring data.

3.1.10 Commonwealth contractors

Outsourcing can be an efficient and effective means for an agency to perform its IT functions. Nevertheless, as a private sector company will have access to information (often sensitive information) collected by the Commonwealth, there is an additional risk to the information, which needs to be effectively addressed.

Until 21 December 2001 the Privacy Act did not directly cover contractors to Commonwealth agencies. The contracting agency (with a few exceptions, including intelligence agencies and government business enterprises) was subject to the IPPs, and in particular to IPP 4(b), which provides:

> A record-keeper who has possession or control of a record that contains personal information shall ensure: … (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything

---

[12] *Privacy Compliance Audit: Commonwealth Government Websites 2001*, Office of the Federal Privacy Commissioner, available at http://www.privacy.gov.au/publications/wsr01.html

[13] In summary, IPP 2 requires that when an agency collects personal information directly from an individual, that the agency takes reasonable steps to ensure the individual is aware of a number of things, including: why their personal information is being collected (for what purpose); if it is being collected as required or authorised by law, the fact that this is so; and those to whom the information may be disclosed.

reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Thus, if a Commonwealth government agency gave an IT contractor access to personal information, one of the things the agency could reasonably do was to ensure that the contract contained clauses obliging the contractor to take the same security precautions (in relation to the information) as the agency was obliged to take.

From 21 December 2001, s.95B of the Privacy Act has explicitly required agencies to take contractual measures to ensure that contractors and subcontractors are bound to comply with the IPPs. From this date also, s.13A (1)(c) of the Privacy Act has provided that a contractor that fails to abide by its contractual privacy obligations has committed an 'interference with the privacy' in relation to the individuals involved. The Commissioner is now able to investigate the contractor directly under s.40 of the Privacy Act.

3.1.10.1 Senate inquiry into IT outsourcing

In February 2001, the Commissioner made a submission to the Senate Finance and Public Administration References Committee's Inquiry into the Government's Information Technology Outsourcing Initiative.[14]

The conclusions of the submission were summarised as:

- Personal information is a basic tool of government operations. Australians provide large amounts of often sensitive information to governments at all levels with a legitimate expectation that it will be accorded a high level of privacy protection;

- The *Privacy Amendment (Private Sector) Act 2000*, which was then to commence on 21 December 2001, should significantly improve the level of protection afforded to personal information held by Commonwealth contractors;

- Under the then existing legislative framework, the use of contracting out had made it more difficult to guarantee that people's information would receive appropriate protection;

- Nevertheless, a measure of protection had been available through the use of appropriate clauses in contracts; and in 1994, the then Privacy Commissioner had issued guidelines setting out model clauses that Commonwealth agencies had been incorporating in their contracts; and

- Experience suggested that few information privacy issues had arisen in connection with the Commonwealth IT outsourcing initiative.

---

[14] The submission is available at http://www.privacy.gov.au/publications/subout.doc

3.1.10.2 Privacy audits of Commonwealth agencies' IT outsourcing arrangements

While the existence of clauses obliging contractors (with access to Commonwealth information) to abide by the same IPPs as the contracting agency, is important, the clauses will not achieve their objective unless the agency makes sure the contractor is abiding by them. To test whether agencies are monitoring contract provisions, in June 2001 the Office conducted audits under section 27(1)(h) of the Privacy Act on:

- The Public Service and Merit Protection Commission (now the Australian Public Service Commission);
- The Health Insurance Commission;
- The Australian Electoral Commission;
- The Aboriginal and Torres Strait Islander Commission; and
- The Department of Immigration and Multicultural Affairs.

Overall, the level of compliance with the IPPs in relation to IT contracting by agencies was assessed as satisfactory. Findings were made with regard to compliance with IPP 4.[15] The main issues arising from the audits related to:

- Contracts with outsourced service providers not containing appropriate privacy clauses;
- Minor physical and logical IT security issues; and
- Some employees of contractors and subcontractors not having executed deeds in relation to privacy.

The last dot point illustrates how important it is that the agency effectively monitors the contractor's compliance with the contract's privacy-related clauses. Clauses that require the contractor's employees to sign deeds, acknowledging their responsibilities in relation to security and privacy, are an important protection for the personal information to which those employees will have access. Such clauses are entirely ineffective if they are not complied with and the deeds not signed. Agencies must not only enter into well-designed contracts, they must take steps to ensure that the provisions of the contracts are put into practice.

---

[15] IPP 4 requires, in general, that agencies protect personal information against loss, unauthorised access, use, modification or disclosure, and against other misuse, by adopting reasonable security safeguards, including doing everything within the agency's power to ensure that service providers handling material containing personal information do not misuse it, or disclose it without authority.

3.2 Emerging issues, trends, developments and challenges affecting privacy, security and data integrity in the Commonwealth

This section discusses some initiatives, information management trends and environmental changes that the Office considers may significantly affect, or are already affecting, individual privacy and electronic information management in the Commonwealth.

3.2.1 National security

In responding to the terrorist attacks in the USA and Bali in 2001 and 2002, the USA, much of Europe and Asia, Canada, and Australia and others, sought to introduce anti-terrorism measures to tighten national security and crime prevention regimes and minimise the possibility of similar future events. Given the scale of the events there was widespread public support for many of these actions. Democracies have been struggling to counter terrorism while trying to minimise the impact on the freedom of their citizens. There has been vigorous debate in Australia over how to achieve the appropriate balance between privacy, liberty and national security.

The Office has been an active participant in this debate, making a submission to the Senate Legal and Constitutional Legislation Committee's inquiry into the Government's proposed legislation seeking to counter threats of terrorism against Australia. Subsequently, the Parliament adopted changes to the legislation that were consistent with many of those proposed by the Office, including narrowing the definition of 'terrorism'.

In its submission, the Office noted that:

> It is easy to argue that security necessarily comes at a cost to liberty. That is, we can only enjoy the right to feel safe and secure if we forgo certain other rights, such as the right to privacy. This is not necessarily the case. It is possible for people to have both privacy and security and they expect their parliament to provide them with both.[16]

The Office's submission proposed a balanced framework to assist in considering the implications of potentially privacy intrusive policy or legislation (see section 4.3). This is one of many areas where it is tempting to reach a conclusion that privacy can and must be traded-off for more overriding objectives – for what is there more important than the security of the nation. Yet, in seeking to achieve this end, privacy need not be unduly sacrificed. Careful consideration of privacy issues in determining and generating responses to threats faced, can result in effective policies and laws that attain a balance with individual privacy.

---

[16] Senate Legal and Constitutional Legislation Committee, Inquiry into Terrorism Bills: Submission from the Federal Privacy Commissioner, April 2002 available at http://www.privacy.gov.au/publications/secleg.doc

3.2.2 Identity fraud and identity theft

Identity fraud or identity theft, that is the use of (or assumption of) another's identity for some benefit, can be a particularly invasive and destructive intrusion into a person's privacy. It can impose grave emotional and financial costs on individuals. It can also undermine public confidence in the security of personal information. The way this challenge is resolved represents a clear choice between privacy invasive options and privacy enhancing options. There is already evidence that the latter kinds of solutions are becoming available.[17]

Given the serious implications of identity fraud (and some of the measures being developed to combat them), this has become an increasingly important issue for the Office. While, at this stage, calls and complaints to the Office about identity fraud or theft remain relatively low, the Office has been considering the problem and discussing it with private sector organisations and government agencies. The challenge is to combat identification fraud while maintaining and promoting peoples' privacy choices.

The use of false identities provides a means for engaging in a wide range of criminal activity. It may also be a factor in terrorism, people smuggling and money laundering. The risk of identity theft also reduces community confidence in the authentication processes used for electronic commerce. The availability of a range of new and more sophisticated technologies seems to be a critical factor in the growth of identity fraud.

There is growing awareness that identity misuse is presenting an increasing threat throughout the world. In Australia, the Commonwealth Attorney-General's Department undertook a scoping study on the proof of identity risks facing key Commonwealth agencies. It canvassed a range of options to improve personal identification practices and to detect and deal with identity fraud.

While the resulting report, *Who goes there? – A Study on the Management of Identity Fraud Risks,* is a protected document; an abridged version (*Scoping Identity Fraud*), available from the Attorney-General's Department, has been prepared to raise overall awareness regarding the issue. It argues that most large, government registers of individuals have inherent data integrity issues due to the lack of standardised proof of identity processes and the apparent ease with which primary identification documents may be forged. The report sets out a number of possible responses, including:

- Random surveys to check the identities of clients of Commonwealth agencies;
- Agencies to agree on those identifying documents that can be regarded as having 'high integrity' and so can be relied upon;
- More on-line checking and verification at the point of registration for Commonwealth services;

---

[17] *Under the Gaze: Privacy, Identity and New Technology*, speech by the Federal Privacy Commissioner, 2002, available at http://www.privacy.gov.au/news/speeches/sp104notes.doc

- A range of data-matching across Commonwealth and State databases; and

- Establishing a Commonwealth Identity Data Agency to carry out some of these strategies.

A report by the United Kingdom Cabinet Office (published in July 2002) provides a similar analysis.[18] It canvasses a similar range of solutions with some notable additions, such as a single 'entitlement card'. The UK Home Office canvasses this latter proposal in detail in a consultation document 'Entitlement Cards and Identity Fraud: Consultation Document', published in July 2002.[19]

The US Federal Trade Commission website (at http://www.consumer.gov/idtheft) also provides a useful compendium of information about identity theft.

The discussion in *Scoping Identity Fraud* acknowledges that privacy is a key factor in dealing with identity fraud issues because:

- Of the impact identity fraud can have on individuals;

- Some of the IPPs in the Privacy Act, for example those involving requirements for personal information to be kept accurate, up-to-date and complete and for individuals to have access to their personal information on request, are part of the solution; and

- Some solutions may themselves be privacy intrusive.

Agencies, including the ATO, NOIE, the Australian Transactions Reports and Analysis Centre (AUSTRAC), the Australian Bureau of Criminal Intelligence (ABCI) are currently involved in a number of parallel activities examining proof of identity, identification and fraud control options.

The Office will continue to encourage the use of balanced frameworks (such as the one included at 'Attachment (c)' or as described in section 3.2.1) when agencies are making assessments about which strategies to adopt. Such a framework may also help encourage a shift in thinking from regarding privacy as only an individualist value that competes with 'genuine' social interests, to an approach where both privacy and *other* social interests can be accommodated to the extent possible.

There is, however, no 'silver bullet' solution to identity theft. While the law (through the Privacy Act) sets out agencies' obligations to secure personal information, this alone is not enough. An effective solution must involve a mixture of law, appropriate security measures, staff training, technology, market solutions and personal action. Indeed, building systems so that by virtue of technology identity fraud *cannot* occur, may be more effective than making laws that say it *should not* happen.

---

[18] Available at http://www.piu.gov.uk/
[19] Available at http://www.homeoffice.gov.uk/dob/ecu.htm

As highlighted in the Privacy Commissioner's paper for the 75th Annual Congress of the Union Internationale des Advocats (October 2002), privacy enhancing technologies are becoming available to assist agencies and private sector organisations in incorporating privacy into their systems and business processes:

> Information technology companies are currently investing considerable resources in developing new technologies which aim to provide the necessary functionality while protecting privacy. Technological means to protect privacy can involve restricting access to privacy related information or the development of systems that provide the necessary functioning without needing to reveal privacy related information. Restrictive tools include cryptographic encoding such as public key infrastructure and digital signatures or systems that simply do not generate the information in the first place. These can be supplemented with technical tools that specify the privacy preferences of individuals.
>
> One new technology which claims to be a PET is IDEMIX[20] developed by IBM. IDEMIX stands for 'identity mix'. This enhanced public key technology tool claims to provide authentication functionality without revealing an individual's identity. In the IDEMIX system organisations only know users by their pseudonyms. The user can have a different pseudonym for each organisation and these different pseudonyms cannot be linked. A key part of IDEMIX is a 'pseudonym authority' which users can access easily and which grants users 'pseudonym credentials'. Most online services generally require you to provide a user name and password to use them. With IDEMIX the user first selects a pseudonym and registers that pseudonym and then receives the corresponding credentials and an electronic signature. If the user then wants to access the service, he or she need only provide proof to the service that that the corresponding digitally signed credentials are in his or her possession. The pseudonym and credentials are given to the online service in an encrypted form and the online service is not able to decrypt them, but they can verify the authenticity of the encrypted pseudonym with the pseudonym authority. A new encryption is used every time the user presents the credentials to another organisation. The system comes with other important controls, including prevention of re-use of information and self-destruction of the data on misuse.
>
> This system and others like it allow for 'pseudonymity' rather than anonymity. In many cases total anonymity may not be appropriate. If the identity of the individual is necessary, for example in an investigation of fraud, the pseudonym authority can uncover the individual user's identity.
>
> Biometric encryption is another new technology with the potential to enhance privacy protection. Biometric encryption uses a person's biometric such as a finger pattern or iris scan and uses it as part of an encryption algorithm to encrypt a PIN number. The finger pattern is not stored and the PIN number cannot be decoded without your live finger pattern. Only the individual with a particular biometric can gain access to an account or computer system. With this system, the biometric cannot be used as a universal identifier as it is used to encrypt a different number or alphanumeric for each

[20] For more information on IDEMIX see www.zurich.ibm.com/security/idemix/

application. There is not one single link as each encryption is different and cannot be matched.[21]

Another example of a potentially privacy enhancing technology is P3P (Platform for Privacy Preferences)[22] - a technical standard developed by the Worldwide Web Consortium (W3C) designed to allow users to set privacy preferences in their browser and prevent access to sites that do not accord with the user's preferences. While this technology does not protect privacy itself, it can enable individuals to make appropriate privacy choices.[23]

3.2.3 Database integrity

The threat of identity fraud, as well as the need for information about individuals to be current and accurate in order to administer government programs, means that Commonwealth agencies need to have greater confidence in the integrity of their databases.

There is evidence that personal information currently held by Commonwealth agencies is of varying levels of integrity. This ultimately affects agencies' abilities to administer their programs effectively. The ANAO and various Parliamentary Committees have criticised aspects of database management and, in particular, the integrity of the personal information held on most government databases.

For example, the House of Representatives Standing Committee on Economic, Finance and Public Administration focussed on data integrity in its report, *Numbers on the Run*, following its review of the ANAO audit report No.37, 1998-99, on the management of Tax File Numbers.[24] The Committee's report identified worrying levels of inaccuracy and duplication in tax file number information held by the ATO and made recommendations similar to those listed in the *Scoping Identity Fraud* document.

In the current environment, many agencies are undertaking individual programs of 'data cleansing' in an attempt to maintain or improve the integrity of the identity data they hold. To do this they are developing various means of ensuring individuals are correctly identified. Some agencies are considering major, cross-agency data-matching activities, as well as various new ways of improving identification and authentication processes.

If we are to find an optimal approach to deal with identity fraud, it is essential that the privacy implications of each option are explicitly and systematically assessed via privacy impact assessments (see section 3.1.5.1).

---

[21] George J. Tomko 'Privacy Threats of Biometrics' presentation to 24th International Data Protection Commissioners Conference September 10, 2002, Cardiff, Wales available at www.informationrights2002.org/presentations/tomko_Workshop_4.ppt

[22] For more information on P3P see www.w3.org/P3P/

[23] *Under the Gaze: Privacy, Identity and New Technology*, speech by the Federal Privacy Commissioner, 2002, available at http://www.privacy.gov.au/news/speeches/sp104notes.doc

[24] Available at http://www.aph.gov.au/house/committee/efpa/tfnaudit/REPORT.HTM

3.2.4 Data sharing between agencies and the re-use of information for other purposes

As agencies' programs develop, and more data is amassed across different program streams, the comparison, collation and analysis of larger, more potent, data sets can become an attractive proposition. Similarly, databases established by one agency for a particular purpose can suddenly appear useful, both to other agencies and private sector organisations, for other purposes.

The recent report of the Management Advisory Committee, titled *Australian Government Use of Information and Communication Technology*,[25] is a government asset. Its value is enhanced when it can be accessed and applied to accelerate and improve decision-making within and across agencies, within the bounds of legislation, security and privacy.

Data-matching activities of various kinds are a prime example of the re-use of Commonwealth data for a new purpose (see section 3.1.6). Other current examples of re-use include:

- Extensive permitted uses (under regulations) of data from the electronic version of the electoral roll by various Commonwealth agencies;

- Use of employment and training information, both across programs and longitudinally, to monitor outcomes for individuals who have received welfare assistance, social support and employment services;

- Moves towards using the national motor vehicle and drivers' licence database (NEVDIS, which provides an interface for all state and territory vehicle and driver information) for commercial (i.e. pay-to-use) verification of identity by private sector organisations;

- The on-line verification of identification and other details using data from State and Territory births, deaths and marriages registers, or through verification against recognised and 'trusted' registrations with centralised agencies such Centrelink (presuming that their identification processes are of the highest integrity);

- The use of identification, change of address or change of circumstances information, that was given to one government program, but is then used for others in the spirit of 'collect once, use many times'.

The intention of such activities is generally to deliver well-planned and well-targeted services with maximum efficiency. In most instances, privacy claims do prevent these activities. Generally, the challenge is to find ways to build trust and community

[25] This document, released by the Government's Management Advisory Committee in October 2002, is available on the website of the Australian Public Service Commission at http://www.apsc.gov.au/mac/technology.htm

confidence by developing new approaches and systems that enhance privacy, while delivering on the desired policy aim.

A recent UK Cabinet Office Report, *Privacy and data-sharing: The way forward for public services*, explores this area in useful detail.[26] It argues that to effectively balance privacy and other policy objectives there are four main principles:

- Using the available data in the most efficient and effective ways possible to achieve the policy goals;

- Adopting the *least intrusive* approach (i.e., where the public sector can achieve improvements in services or efficiency without requiring more data and affecting personal privacy, it should do so), thus recognising that the protection of privacy is itself a public service;

- Wherever possible, and where the benefits of the better use of personal data accrue to people using the service, giving citizens more choice in the management and use of their personal data during the delivery of public services; and

- Ensuring that where data are used or shared without the consent of the individual (for example, in law enforcement), there is adequate openness, transparency and consultation in the policy-making process that strikes a balance between individual rights and the wider public interest.

The report also highlights the need for the systematic consideration of privacy (by way of a privacy impact assessment) in decision-making about the need for increased data use or data-sharing. The criteria suggested in the paper reflect other, similar criteria identified elsewhere in this paper and include:

- Assessing the benefits of the proposed data use/data-sharing in meeting public policy objectives;

- Considering alternative approaches to achieving the objectives, which have a lesser impact on privacy;

- Identifying the costs and risks of increased data use/data-sharing, recognising that many of the risks to privacy will be difficult to quantify;

- Assessing safeguards that would minimise the risks (for example, using privacy enhancing technologies);

- Using the accumulated evidence to strike a balance between the benefits and risks; and

---

[26] *Privacy and data-sharing: The way forward for public services*, UK Cabinet Office, April 2002, UK www.piu.gov.uk/2002/privacy/report/index.htm

- Where increased data-sharing is proposed, after this analysis, policy makers should be able to explain why the public interest will be furthered by the proposal, and to demonstrate that the proposed action is a proportionate response to the public policy objective identified.

3.2.5 Trend toward greater identification in electronic transactions

A threshold privacy issue is the trend toward greater levels of identification in many aspects of our lives, including in relation to on-line dealings.

One of the effects of some new technologies has been a loss of anonymity in many transactions conducted electronically. Many electronic transactions, as currently designed, leave digital trails, where the transactions were once anonymous. Hence, in our dealings we are increasingly identifiable as more information is gathered, collated and linked to us as individuals. Despite this tendency, the loss of anonymity is not inevitable. It is technologically possible to conduct anonymous, or near anonymous, electronic transactions – much work is going into develop these alternatives.

Loss of anonymity is often an artifact of the design of new technologies, even where this is not essential to their functionality. When individual anonymity should be retained or eliminated is a matter for public policy through democratic processes, the construction of smarter business models and the design of supporting technologies; it is not a technological or social imperative.

Identification and authentication are important processes that are essential in some circumstances, and privacy is not about promoting illegal activity under cover of anonymity. Yet, the social decisions we as a community make about when and how we need to be identified will have a major impact on the lives and liberties of all Australians, including how we relate to each other and to government. These are most important issues and, as it may be too late to make changes once identification systems are introduced, it is vital that we openly consider the paths available to our community, and transparently choose the one we are going to use.

Some other strategies currently under consideration for dealing with improved identification and authentication include:

- The collection of large amounts of data about particular transactions, over long periods of time. The aim here is to find patterns of behaviours that will help to detect which transactions are fraudulent and which are legitimate. This could mean lots of extra information (such as individuals' addresses, contact numbers and detailed lists of transactional information) would be collected, stored and analysed by companies and law enforcement bodies; and

- Stronger identification measures involving a 'cradle to grave' universal identity card, number or system, which in its most extreme form could involve babies being tagged with a biometric identifier (e.g., a finger print, iris scan or DNA sample), which is then attached to an identity card.

Proposals such as these appear to ignore developments in technology and to avoid careful analysis of the problems that need addressing. Distinctions can and should be made between problems that require identification, or authentication, or merely require irrevocable authentication (see the following section for more information on these terms).

A single card with one number to identify one person in all circumstances is not the answer. This is an outdated response with the potential to be privacy invasive. Relying on one unique identifier, used in a whole range of contexts and then able to be linked to a range of information is an approach that permits unrestricted identification of patterns of behaviour, and creates unnecessary privacy risks.

Identity authentication systems that do not require an authenticating body to hold large amounts of information about each individual, and where the individual knowingly exercises a choice to enroll in the system, pose less risk to privacy, while being able to authenticate their data subjects (see the information on pseudonymity in section 3.2.2, p. 31).

In finding an appropriate balance between privacy and individual accountability, it is essential to distinguish between circumstances where 'full identification' is required and those where only 'authorisation' is needed. When developing privacy enhancing technologies, it is vital to determine when knowledge of a person's identity is necessary and when it is not, and then to build systems that make an appropriate distinction between the two.

3.2.6 Anonymity, Identification and Authentication

Anonymity is not synonymous with privacy; it is one means by which individuals can exercise privacy choices. Privacy can be said to have three elements:

- What is known about a person;
- Whether there is physical access to the person; and
- Whether attention is paid to the person.

The last of these is relevant to anonymity. Anonymity can mean being unacknowledged as well as being unidentified.[27]

Complete privacy and complete anonymity are neither possible, nor desirable, in human society. A free society, however, allows individuals to make choices within certain parameters about when, and to what extent they reveal themselves to others; requiring

---

[27] Ruth Gavison 'Privacy and the Limits of Law', *Yale Law Journal*, 1980, Vol. 89 pp. 421-471 quoted in Diane Rowland, 'Anonymity, Privacy and Cyberspace' paper presented to the 15th Bileta Conference: *Electronic Datasets and Access to Legal Information* Friday 14 April 2000, University of Warwick, Coventry England available at www.bileta.ac.uk/00papers/rowland.html

individuals to identify themselves, when this is not necessary, results in privacy intrusion. While there are circumstances where it is necessary to ensure that a person is who they say they are; there is also considerable confusion between this and when a person need only authenticate something about him or herself to satisfy requirements for a given transaction.

Furthermore, identification and anonymity are not binary opposites; rather they reflect the different ends of the same spectrum with many shades of grey connecting them.

To more carefully consider issues around identification, an important distinction needs to be made between identity and identification:

- Identity is complex and multifaceted. Each of us has a range of different identities defined through things such as our relations with others; our position or status within the workplace, the family, community or society; our actions, behaviours, characteristics or attitudes; or the circumstances of the moment; and

- Identification is the *action of being identified*, of linking specific information with a particular person. An individual's identity is fluid and changes over time. The extensive linking of different information about an individual, to try and capture an immutable or essential identity, can be both inaccurate and restricting to this fluidity. To allow for growth and development, individuals need to change and move through life, during which time, what identifies a person can change. For example, few of us want to be defined forever by the characteristics we displayed at the age of 17.

While identification can potentially relate to a wide range of elements in an individual's identity, most easily in practice, identifying an individual generally involves focusing on those things that distinguish the individual from others. This can include their legal name, date of birth, location or address and symbolic identifiers such as a driver's license number. The basis for identifying a person can also involve:

- The person demonstrating that:
    - They have knowledge of something (e.g. a password); or
    - They possess a token (e.g. driver's license); or
- A person's physical appearance, their actions or characteristics (e.g. facial features, signature, fingerprint); or

- A person's social characterisation (e.g. their gender, ethnicity, education, employment and leisure activities).

One of the effects of many new technologies is the emergence of 'identity creep' – the capacity for organisations to achieve identification of individuals using 'non-identified' information through powerful data mining tools that link previously unrelated data items. This collection, collation and linkage of seemingly innocuous data, rather like piecing together the clues in an identity game, can unexpectedly result in our being identified

when we may not expect it, and when we thought that information arising from a range of choices and transactions was unrelated and unconnected. These developments lead to individuals losing not only choice and control over when they are identified, but also knowledge and understanding about how and when they have been identified (or profiled) and by whom.

3.2.6.1 Defining identification, authentication and authorisation

There is a significant distinction to be made between the processes of identification and authentication.[28] A transaction may involve a number of elements, including authorisation, identification and authentication. It is necessary to explore these concepts a little more to understand their importance for privacy.

'Identification' means the process of accurately identifying a person, thus ensuring that they are who they say they are. This generally involves checking documentation, such as records for the basis of identification criteria like those listed in the previous section.

'Authentication' involves checking an assertion made by a person. Authentication can include confirming that a person seeking to make a transaction is the same person who opened the account. Authentication may also include, however, other assertions, such as merely the fact that the individual holds a valid driver's license, or is offering a valid payment, but without the organisation needing to know anything more about them. Often an individual's identity is not at issue during a transaction, and some other claim they make is more important.

We take **'authorisation'** to have two stages. Firstly, the initial allotment of privileges to a person, for example the allocation of a user representation such as a bank account number. The second stage can be called 'access control', where the organisation's information system checks whether the user representation is authorised for each service provided.

For the organisation, the structure of a transaction generally involves: prior authorisation to undertake a transaction of this type, a process of authenticating the user representation (for example, checking a PIN number against a particular automated teller card), and then a process of access control or a specific authorisation for the particular transaction. Authentication may or may not require the more complete identification of the individual.

From the individual's perspective 'authorisation' is the act of authorising a transaction. This may or may not need to reveal their identity. For instance, paying for goods with cash may not require any identification, whereas the same purchase with a credit card at least involves sufficient data to establish the authorisation to use the credit service.

---

[28] Roger Clarke 'The Mythology of Consumer Identity Authentication' (Paper for 24th International Conference of Data Protection & Privacy Commissioners, Cardiff UK 9-11 September 2002) available at http://www.informationrights2002.org/presentations/clarke_Workshop_5.ppt

Distinguishing between identification, authentication, and authorisation requires clarity about the real purpose for the collection and use of the information. There are new technologies with the capacity to enable authorisation and authentication in transactions without revealing identity.[29] It is important, therefore, to be wary of collapsing all authentication and authorisation processes into identification, so that where the latter is not required individuals are not forced (by system design) to provide it.

Innovation and the up-take of new identification/authentication processes are inhibited by the lack of an agreed set of standards, for both the public and private sectors, for minimum requirements for privacy and security in this context. The development and promulgation of such standards will provide a means through which agencies and organisations can more confidently determine whether new technologies or models can be appropriately adopted in the course of their business. A coordinated approach in this area, driven by a central, expert body such as the Information Management Strategy Committee, would be of significant benefit both to new technologies and to privacy.

Recommendation 4:

That the Committee endorse the approach announced by the newly established Information Management Strategy Committee (IMSC) to lead a coordinated, cross-Commonwealth initiative on electronic identification/authentication and proof of identity issues. The Committee should give consideration to recommending that the Privacy Commissioner be co-opted as a member of the IMSC to ensure the necessary consideration of privacy.

The IMSC should be well resourced in order to properly consider privacy, including by investing projected savings (both savings arising from the reduced incidence of fraudulent identity and its implications for government, as well as the efficiencies generated through the reduction in duplicated services) into the building of a privacy-enhancing identification/authentication mechanism or approach.

The IMSC can take a key role in resolving one of the major inhibitors to the development of new identification/authentication models in both the public and private sectors, by leading work toward an agreed set of standards that will set the benchmark for the necessary privacy (including security) requirements of all new initiatives in this area.

---

[29] For more on this topic see the Commissioner's paper titled *Under the Gaze, Privacy Identity and New Technology* http://privacy.gov.au/news/speeches/sp104notes.doc

3.2.7 Government policy for on-line government and E-commerce

For a number of years, the Government has been pursuing strategies to promote and encourage the uptake of electronic and on-line dealings in both the public and private sectors. This requires the provision of an appropriate legal framework, the development of standards, skills and knowledge, and systematic attention to privacy and security. NOIE is currently the agency with primary responsibility for many of these strategies.

A notable initiative in this area is the new governance and investment framework for Australian government use of information and communications technology recently decided upon by the Management Advisory Committee (which advises the Government on matters relating to the management of ICT strategy across the Commonwealth).[30]

3.2.8 Health sector initiatives

In the area of health information, governments at Commonwealth, State and Territory levels are exploring the possibilities for electronic health records. Given the community's view that health information is some of the most sensitive information about a person, developments in this area require close consideration. Here is an opportunity to develop privacy and security solutions of a very high standard, because the community will accept no less in how its health information is handled, and there is much impetus to improve information management within the health sector.

With key initiatives such as Health*Connect* (a joint Commonwealth, State/Territory project) and the Better Medication Management Scheme, which aim to span the public and private health sectors, the centrality of privacy protection in the 'build' of each system cannot be understated. Without good privacy protections, health consumers will avoid such systems. By contract, effective solutions in these areas could set new benchmarks in identifying/authenticating individuals, managing and securing data, and in making sure that consumers retain control over how their data is handled.

The pace of development in the e-health area also provides opportunities to lead on other privacy issues, such as the identification/authentication of health consumers. Hence, as old solutions to such issues become outmoded and ineffective due to data integrity challenges and the relative ease of fraudulent duplication (such as the provision of a unique number on a magnetic swipe-card), so other identification/authentication options demand consideration. If these are innovatively developed to successfully meet current day data management challenges in health privacy, then the successful solutions could be adapted to deal with similar issues for purposes as broad as national security, border control, taxation and law enforcement.

---

[30] For more information, see the Information Management Advisory Committee website at http://www.imsc.gov.au/

Health agencies have generally recognised early that privacy is a key issue in developing systems that Australians will be willing to use. Strategies are in place aimed at building privacy into systems development including though extensive consultations with the Office and providing the Office with additional resources so that it can participate in the debate, as well as developing privacy expertise within key agencies and undertaking extensive public consultation on core issues.

3.2.9 Cross jurisdictional service provision and the Government one-stop shop approach

Another trend in government service delivery that relies on good quality data (and raises issues similar to those identified in relation to the re-use of data or the levels of identification needed in transactions, see sections 3.2.4, 3.2.5 and 3.2.6) is the use of a common electronic portal to access services across a range of agencies and even, perhaps, across different levels of government.

This trend is driven by a desire to provide seamless and personalised government services, and the increasing understanding that it is not easy for individuals to understand and navigate between the various arms of government.

To date, a number of pilot projects are being trialed in various jurisdictions. For example, NOIE is sponsoring a demonstration project in Tasmania – the Trials of Innovative Government Electronic Regional Services (TIGERS).[31] Through the use of new technology, governance and management arrangements, TIGERS is conducting a series of individual trials aimed at making it easier for customers to do business with Commonwealth, State and Local Governments.

TIGERS' program activities include the development and implementation of a variety of integrated, cross-jurisdictional government services and research projects. As a demonstration program, TIGERS will share the knowledge and learning gained during the trials, and will seek to facilitate the take-up of successful service delivery models by other jurisdictions in Australia.

While this trend has the potential to make interactions with government easier and more intuitive, it also has the potential to be intrusive. The difference in outcomes is likely to depend on factors such as:

- The extent to which participation is voluntary and people have real choices about which personal information they wish to share with which agency and whether they have alternative means for doing business with the agency;

- Whether the collection of identified information is limited to that necessary to deliver a particular service or services; and

[31] For more information on TIGERS, there is a Fact Sheet on the NOIE website at http://www.dca.gov.au/nsapi-graphics/?MIval=dca_dispdoc&ID=3954

- The extent to which systems are designed to support peoples' privacy choices, including ease in the use of electronic interfaces and the stringency of security measures.

These kinds of cross-jurisdiction activities also raise similar issues as emerged with the establishment of Centrelink (see section 3.1.7), such as: which regulatory framework (including privacy framework) will apply; who 'owns' the data and so is responsible for its protection; who can use/disclose data and under what rules. It is vital to gain clarity around these issues so that data can be managed effectively, and complaints or investigations/audits handled properly.

3.2.10 The privacy challenge

The privacy challenge for agencies is to consider and deliver good privacy protections when they propose and then deliver on new projects or initiatives, such as those discussed in this submission.

Ensuring that accurate, easily understood and timely advice on new data use developments is provided to stakeholders or customers, as well as the community more generally, is a vital step in ensuring privacy compliance. One of the keys to good privacy for Commonwealth agencies is ensuring that people know why their personal information is being collected, how it will be used and to whom it may be disclosed. This advice is usually contained in an agency's 'IPP 2' statement. This is often found on the forms used for collecting data or on related information pamphlets or a relevant website.

Similarly, community expectations need to be considered and widespread consultation undertaken when new uses of data are being considered. With ever-easier and cheaper options for manipulating data, there is greater potential for data-matching and profiling individuals in new ways. Agencies need to consider the implications for the community, and how these relate to community expectations about how previously collected data would be used.

The gradual metamorphosis of data-handling objectives can quickly lead to 'function creep'. Without adequate consultation, the community can easily loose touch with how an existing program or initiative operates and how their data will be used. This represents not just a privacy risk, but a broader risk to the level of confidence the community and key stakeholders have in the agency and its programs. In turn, this could jeopardise the objectives of the project and the agency. It is vital, therefore, to build strong privacy protections into new projects and systems by ensuring that people know what is proposed and how it will work, gauging community expectation, maintaining real choices for individuals, and effectively managing data security and integrity.

3.3 The adequacy of the current legislative and guidance framework

The Office considers that, generally, the current privacy framework is adequate, though there are emerging calls by privacy and legal commentators over recent years for a discussion on the need for new privacy principles.

At this stage, however, the Office considers it important to highlight some specific areas where improvements in practice, law or guidance may be warranted given recent developments in the management and handling of personal information in the Commonwealth sector.

3.3.1 Privacy Contact Officers

The Office has long encouraged Commonwealth agencies to nominate a Privacy Contact Officer (PCO) to facilitate the agency's compliance with the Privacy Act. The majority of large agencies, and many of the smaller ones, now have a nominated PCO – some have groups or teams of PCOs. The Office engages with PCOs on particular policy and operational issues, as well as through a network, but is continually seeking to improve the ways in which it can assist and support PCOs.

The Office is seeking to establish a model whereby PCOs are:

- The first point of contact for discussion and consideration of privacy issues within their own agency;
- The first point of contact, or a coordinating point for privacy complaints made directly to the agency;
- The main contact point between their agency and the Office;
- Responsible for reporting potential breaches of privacy to the Office; and
- Responsible for educating their agency on its privacy obligations and the implementation of privacy practice.

This role could extend to include strategic advice on the privacy implications of new information management systems or approaches. This already occurs in some agencies, but is not the norm.

PCOs are variously resourced in many ways, including in the proportion of time they can devote to privacy issues, their level of seniority and decision-making or advising authority, the level of training they receive on privacy issues, and the extent to which there is agency recognition and acceptance that privacy issues are at stake across all agency functions involving personal information.

In 2001, the Office surveyed some aspects of the implementation of privacy in Commonwealth agencies.[32] Responses from non-PCOs suggested that full use was not being made of PCOs within their agencies – PCOs ranked third when respondents were asked to choose their main source of privacy advice.

Regarding electronic databases, for instance, it may be highly beneficial to have PCOs brought into agencies' development processes earlier. In some agencies, this may require some 'skilling up' of PCOs, as there appears to be a weighting toward legal rather than information and communications technology (ICT) skilled officers. Interestingly, in the 2001 survey, PCOs ranked on-line service delivery and database management as two key areas from a proposed list of eight challenges to their privacy responsibilities.

Recommendation 5:

That agencies be expected to continue to have a Privacy Contact Officer (PCO), including a commitment by each agency to the importance of the role, with the necessary seniority and level of resources available to underpin the effective operation of the role.

3.3.2 Regulator issues and resources

As noted, the Office and the ANAO both have roles in auditing Commonwealth agencies' privacy practices. These roles can overlap from time to time as the ANAO examines practices of Commonwealth agencies during performance audits (and in some cases this may include looking at whether personal information is being handled by an agency in accordance with the IPPs). Both offices are aware that this overlap can create difficulties, especially if an agency is asked to comply with requirements placed upon them by different regulators. For example, a best practice recommendation from a performance perspective (made by the ANAO) might not be best practice in terms of protecting the privacy of individuals under the Privacy Act (as stated by the Office).

The Office and the ANAO consult regularly in order to minimise overlap in their roles, taking into account the legislative functions and obligations of both agencies, and the resource constraints upon the Office. Within the statutory parameters, however, the arrangement is working well.

The ANAO has expressed interest in the Office observing the planning sessions for the next ANAO audit program, and on advising the ANAO of areas within the operations of particular agencies that the Office might itself audit. The ANAO has indicated a willingness to expand its fieldwork to look at identified issues as part of performance audits. This approach would also benefit the ANAO in developing its expertise in the privacy obligations of agencies, to better ensure that these are taken into account in recommendations the ANAO might make in its audit process.

---

[32] *Privacy and Government*, Office of the Federal Privacy Commissioner, July 2001, available at http://www.privacy.gov.au/publications/rgovernment.html

3.3.3 Guidance available on privacy, security and data integrity

The Office considers that more guidance may be needed in relation to some specific aspects of data security and integrity, and that this might be achieved through a whole-of-government approach in line with framework set in place by the Management Advisory Committee report *Australian Government Use of Information and Communications Technology: A New Governance and Investment Framework* (October 2002).[33] For instance, more guidance on data security may be necessary to ensure that agencies fulfil their obligations to ensure that personal information they hold in their IT environments is protected, including through safeguards in accordance with the Protective Security Manual (PSM) and ACSI33.

The Protective Security Coordination Centre (PSCC) in the Attorney-General's Department is responsible for the PSM; it educates agencies about security measures and can investigate breaches of the PSM. ACSI33 is a set of standards for security measures, and the Defence Signals Directorate (DSD) has a role to provide agencies with advice on how to meet those standards.

By way of example, the Office itself encountered some difficulty when trying to comply with the *Electronic Transactions Act 2000* – so that individuals can lodge privacy complaints electronically (and securely), if they choose to do so. The Office approached DSD for advice about encryption software that had been examined and approved as suitable for use by agencies for these purposes – but was advised that no such software had been approved.

In the meantime, the Office has instituted an arrangement using 'hushmail' that improves security without providing any guarantees. The individual has to make their own assessment on whether to use it.[34]

Recommendation 6:

That the gap in guidance between the Information Privacy Principles (in the Privacy Act), the Defence Signals Directorate (DSD) and the Commonwealth Protective Security Manual (PSM) be filled by more practical, operational guidance. For example, an on-line authentication guide developed by an agency such as the National Office on the Information Economy (NOIE) in association with the Office.

---

[33] Access to this report is available via the Australian Public Service Commission's site at http://www.apsc.gov.au/mac/technology.htm

[34] For more information on making complaints to the Office see the following web pages: http://www.privacy.gov.au/privacy_rights/complaints/index.html#complaint and http://www.privacy.gov.au/privacy_rights/complaints/index.html#send

Recommendation 7:

That the Office be resourced to discharge the additional functions arising from the implementation of these recommendations.

3.3.4 Health Privacy Regulation

With the privacy of health information an area of significant concern to the Australian community, the handling of such information needs high standards. This is reflected in the private sector amendments to the Privacy Act. Recognition of the need for additional protection for health information means that the Privacy Act is a sound basis from which to build a more comprehensive regulatory scheme for the protection of health information.

Presently, data is protected under the Privacy Act when it is held and handled by Commonwealth health agencies (eg. the Health Insurance Commission and the Department of Health & Ageing), and equally when it is handled by private sector health service organisations.

As electronic health initiatives develop, and given the cross-jurisdictional nature of the health system between the Commonwealth, the States/Territories and the private sector, building upon the Commonwealth privacy scheme to provide a nationally consistent scheme across the country, is a vital development. This matter has been under consideration by a Privacy Working Group, set up by the Australian Health Ministers' Advisory Council, since 2000. A nationally consistent approach is pivotal in ensuring effective health privacy for all Australians across all facets of the health sector.

With a consistent set of rules nationally, and additional privacy features (such as penalties for breaches to health privacy, or the inclusion of other information-handling issues specific to health service provision) being added to the central framework, then building on what works today can deliver a more comprehensive system to meet future challenges.

4 Background information

4.1 Terms of Reference of the Inquiry

'The Committee shall inquire into and report on the potential risks concerning the management and integrity of the Commonwealth's electronic information.

The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. Various Commonwealth agencies and private bodies acting on behalf of the Commonwealth hold this information. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information. The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

In conducting its inquiry the Committee will consider:

- the privacy, confidentiality and integrity of the Commonwealth's electronic data;
- the management and security of electronic information transmitted by Commonwealth agencies;
- the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and

the adequacy of the current legislative and guidance framework.'

4.2 Privacy: a brief history, current privacy regulation in the Commonwealth sector, and the role of the Office of the Federal Privacy Commissioner

Australians hold strong opinions about privacy. The results of many surveys, including two undertaken by the Office in 1995 and 2001, give a clear indication about the strength of feeling of our community about privacy, including the areas where people think that privacy is most important.[35]

The contexts in which privacy has emerged as a 'top of mind' issue are diverse, including for example Australia's response to the 1986 proposals for a national identity card (the Australia Card), and more recently, evidence that concern about privacy is one of the major barriers to up-take of E-commerce services. This indicates that there are many dimensions to privacy and that the community's issues and concerns in this area change over time and with context.[36]

Both examples also remind us that privacy as a right and/or a community value is usually (probably always) one part of a wider debate, involving other objectives and values – such as, fraud control, the free flow of information for business and government, or the need for a safe society – and all must be balanced to attain a workable and balanced society.

In considering how and where privacy takes its place in a workable society, it is worth briefly reflecting on the question: 'what is privacy?'

In 1890, in a key, early writing on privacy, Samuel Warren and Louis Brandeis popularised Judge Cooley's suggestion that privacy is the 'right to be let alone'[37] and argued for the need for a legal protection of this right in the face of 'recent inventions and business methods'.

While the world and business methods have changed since the late-nineteenth century, the Warren and Brandeis formulation remains one of the simplest and perhaps most meaningful approaches to understanding 'what privacy is'.

---

[35] Available at http://privacy.gov.au/publications/rcommunity.html,

[36] *Current State of Play*, NOIE, 2000 - Intensity - International Benchmarking - Business to Consumer (http://www.noie.gov.au/projects/framework/Progress/ie_stats/StateofPlayNov2000/intensity/intensity_7.htm)

[37] Samuel Warren and Louis Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* 193, 1890, and available at www.louisville.edu/library/law/brandeis/privacy.html. They credit Judge Cooley in his *Torts* (2nd Edn, 1888, p. 29) with the phrase 'the right to be let alone'.

Privacy is a fundamental part of human dignity. It is part of the claim for personal autonomy. It supports the various freedoms that democratic countries value, and as then Professor Zelman Cowen said in the 1969 Boyer lectures:

> A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars.38

The Universal Declaration of Human Rights (1948) and the subsequent *International Covenant on Civil and Political Rights* are among a number of international instruments that recognise privacy as a basic right.[39] [40] Article 12 of the Universal Declaration states that (and this is echoed in Article 17 the International Covenant):

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The Australian Law Reform Commission's report on privacy, from its inquiry of the early-1980s, also discusses privacy as part of the claim for personal autonomy.[41] The report cites the example of the interest a person has in ensuring that their body is not interfered with, without their consent.

The claim for personal autonomy is also a claim for control over the way in which we interact with others. This implies an ability to exclude others from our conversations, and to prevent others from spying on our activities. It also includes the interests we have in controlling our personal information.

David Banisar, of the Electronic Privacy Information Centre (EPIC), suggests that privacy can be divided into four separate, but related, concepts:

- Information privacy – involving rules for the handling of personal data;
- Bodily privacy – the protection of our physical selves against invasive procedures;
- Privacy of communications – the security and privacy of mail, telephone and internet communications; and
- Territorial privacy – setting limits on intrusions into domestic and other environments.[42]

---

[38] Zelman Cowen, 1969, 'The Private Man', The Boyer Lectures, Australian Broadcasting Commission, p9-10

[39] Available at http://www.un.org/Overview/rights.html

[40] Available at www.unhchr.ch/html/menu3/b/a_ccpr.htm

[41] The law Reform Commission, Report No. 22: Privacy, 1983,Volumes 1 and 2

[42] Banisar D, 2000, *Privacy and Human rights: an international survey of privacy laws and developments*, Electronic Privacy Information Centre, Washington. www.privacyinternational.org/survey/

The Privacy Act deals mainly with the first of these concepts. It provides a legal framework, in the form of high-level information-handling principles, as well as complaint-handling, investigation and enforcement powers relating to breaches of privacy, to protect and promote the community interest in privacy. The Act also requires the consideration and balancing of privacy in a broader context and with other important interests, both at the policy and systems development stages for government and business.

4.2.1 Privacy legislation in the Commonwealth public sector

The Privacy Act was passed by the federal Parliament at the end of 1988. It initially had a two-pronged objective: the protection of personal information held in the Commonwealth public sector; and the creation of safeguards for the collection and use of tax file numbers (the latter development arose due to the up-grading of the tax file number system following the demise of the Australia Card proposal).

The *Privacy Amendment (Private Sector) Act 2000* extended the Privacy Act to apply to many private sector organisations from 21 December 2001, with some small businesses also brought under its jurisdiction from 21 December 2002. In extending privacy regulation to the private sector, the Government's objective was to establish a single, comprehensive national privacy scheme to meet Australia's international obligations relating to privacy, and to facilitate the uptake of E-commerce.

Apart from the new provisions regarding contracted Commonwealth service providers (see section 3.1.10); the private sector jurisdiction is not described in this submission given the terms of reference of the Committee's Inquiry. Introductory information about the private sector jurisdiction can be found on the Office's website at http://www.privacy.gov.au/act/index.html.

4.2.1.1 The Information Privacy Principles

The IPPs in the Privacy Act set out strict safeguards for personal information handled by Commonwealth and ACT government agencies. These rules cover the collection, storage, use and disclosure of this information.

The IPPs are based on privacy principles developed by the Organisation for Economic Cooperation and Development (OECD)[43] and set out in the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD principles, in summary, are:

- Data should be obtained by lawful and fair means and where appropriate with the knowledge or consent of the data subject;

[43] Available at www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-nodirectorate-no-no-10255-29,00.html

- Personal data held should be relevant to the purposes for which it is to be used and kept accurate, complete and up-to-date;

- The purposes for which the personal is collected should be specified no later than the time of collection, and it should only used be for those purposes or for other compatible, specified purposes;

- Personal data should not be disclosed or used other than for the specified purposes, except with the consent of the data subject or by the authority of law;

- Personal data should be protected by reasonable security safeguards against the risks of loss or unauthorised access, destruction, use, modification or disclosure;

- There should be a general policy of *openness* (our emphasis) about practices and policies relevant to personal data; and

- An individual should have the right to ascertain whether a data controller has data relating to him or her, and to gain access to that information on request and without excess charges. If access is denied, the reasons should be given to the data subject, who must be able to challenge the denial. A data subject must be able to correct or erase inaccurate information.

4.2.1.2 Tax File Numbers

The Privacy Act and the *Tax File Number Guidelines* issued by the Privacy Commissioner provide protection for individuals' tax file numbers (TFNs).

Together, the Act and the Guidelines:

- Prevent the use of the TFN as a national identifier;

- Limit the circumstances in which TFNs can be used and disclosed (by agencies and others) to those uses and disclosures set out in law;

- Give individuals the right to choose whether or not to provide their TFN in a particular transaction. Although, this does not prevent consequences following a choice not to provide a TFN if it is requested (e.g., not receiving a benefit, or having tax withheld at the highest marginal rate).

4.2.1.3 Additional Commonwealth legislation

The Privacy Commissioner also has functions under other pieces of Commonwealth legislation, including:

- The *Data-Matching Program (Assistance and Tax) Act 1990*, which regulates data-matching between the ATO and four assistance agencies, to detect overpayments of benefits and ineligibility for assistance. Under the Privacy Act, the Privacy

Commissioner is responsible for issuing guidelines in this area, and for protecting privacy, investigating complaints and monitoring agency compliance;[44]

- The *National Health Act 1953*, under which the Privacy Commissioner is required (see s.135AA) to issue guidelines covering the storage, use, disclosure and retention of individuals' claims information under the Pharmaceutical Benefits Scheme and the Medicare program.[45]

4.2.2 Role of the Office of the Federal Privacy Commissioner

The Office is a Commonwealth government agency established to support the Federal Privacy Commissioner in promoting an Australian culture that respects privacy. The Office is located in Sydney, with a small staff in Canberra.

The Privacy Commissioner and staff:

- Promote an Australian culture that respects privacy;
- Advise individuals about their privacy rights;
- Give advice to Commonwealth and ACT agencies, private sector organisations, credit providers, credit reporting agencies and others, about their obligations under the Privacy Act;
- Issue guidelines to aid and direct organisations and agencies in implementing the privacy principles;
- Investigate complaints that fall within the Privacy Commissioner's jurisdiction;
- Conduct audits of agencies and organisations that are subject to the audit provisions of the Privacy Act;
- Consult widely regarding peoples' and organisations' understandings, expectations and behaviours in relation to privacy; and
- Provide information to the community about privacy and related legislation.

[44] These guidelines are available at http://www.privacy.gov.au/publications/p6_4_21.doc
[45] These guidelines are available at http://www.privacy.gov.au/health/guidelines/index.html#2.8

4.2.2.1 Privacy Act enforcement and the Privacy Commissioner's powers

The Privacy Act places obligations on Commonwealth agencies to comply with the IPPs. The first and most effective method, of enforcement is the approach to compliance within Commonwealth agencies.

The Act provides for two strands of compliance activity external to agencies:

- It facilitates the consideration of privacy issues at the level of new policy and legislative development (by giving the Privacy Commissioner a role in providing advice and examining enactments where there may be a risk to privacy; and

- And it provides mechanisms to identify, and deal with, complaints and systemic failures in personal information-handling practices.

4.2.2.2 Examining enactments and providing privacy advice

In summary, section 27 of the Privacy Act provides the Privacy Commissioner with functions to:

- Examine (with or without a request) enactments that may have an adverse affect on the privacy of individuals; and

- Provide advice (with or without a request) on any matter relevant to the operation of the Act.

In relation to the former function, the Cabinet Handbook and the 'Drafter's Guide' (issued by the Department of Prime Minister & Cabinet) alert agencies to the need to consult the Privacy Commissioner on matters to be proposed in Cabinet Submissions, Cabinet Memoranda or legislative proposals, where there are privacy implications.[46]

Agencies consult the Office about matters such as those noted in the 'Drafter's Guide', as well as about operational privacy issues.

The extent to which the Office is able to respond to agency requests for advice depends on the resources available at the point it is consulted. The Office's involvement varies from participation in working parties and attending meetings, to providing detailed submissions, providing Cabinet Submission coordination comments or providing advice on particular agency issues.[47]

---

[46] More information available at http://www.dpmc.gov.au/docs/displaycontents1.cfm?&ID=101

[47] It is the area of individual requests for advice to agencies on new practices and proposals that require assessment and prioritisation by the Office, and it is in this area that agencies' Privacy Contact Officers can be most valuable (see section 3.3.1).

4.2.2.3 Complaints investigation

The Privacy Commissioner has powers to investigate complaints received from individuals about an alleged interference with privacy that involves a breach of the IPPs. The Office first attempts to resolve complaints through conciliation by seeking to find a mutually acceptable solution for the individual and the respondent agency.

If conciliation fails, the Commissioner can make findings regarding whether a breach of the Act has occurred. If so, Commissioner may set out the remedies that are considered appropriate under the circumstances. If an agency refuses to accept a decision of the Commissioner, either that a breach has occurred or that certain remedies are appropriate, then the Commissioner may make a Determination (under section 52 of the Act), which can include declarations as to steps the agency must take, including financial compensation to be paid to the complainant.

Section 58 of the Act obliges an agency to comply with declarations made by the Commissioner in a Determination. If the agency fails to do this, the Commissioner (or the complainant) may seek enforcement of the Determination in the Federal Court or the Federal Magistrate's Court.

4.2.2.4 Own motion investigations

Where the Commissioner learns about the actions of a respondent that may constitute an interference with the privacy of individuals, then he may commence an investigation of his own volition.

The powers attached to such investigations are not as full as those attached to complaints from individuals. Under section 30 of the Act, however, if the Commissioner thinks that an act or practice of a respondent, including an agency, is a breach of privacy, and decides that it is not appropriate to try to effect a settlement with the agency (or has tried without success), the Commissioner must report the matter to the relevant Minister. The Commissioner may, if he chooses, also provide a report to the relevant Minister in cases where a resolution is found.

4.2.2.5 Audits

The Commissioner has the discretion, set out in section 27(1)(h), to audit agencies to assess their compliance with the IPPs (and the *Tax File Number Guidelines* under s.28(1)(e)).

While the audits conducted by the Office are 'compliance audits', the approach taken is an educative rather than a punitive one. The Office makes recommendations to an agency about how it can improve its privacy compliance, and thereby better protect the personal information of Australians.

The audit process involves:

- Based upon information gathered during fieldwork at an agency's premises, the Commissioner provides the agency with a list of preliminary compliance issues (at the completion of the fieldwork);

- the Commissioner then issues a draft report to the agency containing findings of potential breaches of the Act and recommended action/s to minimise the identified risks; and

- The responses from the agency being incorporated into the Commissioner's final audit report, along with any further comments from the Office.

While the Privacy Act is silent on whether audit reports may (or should be) published, from this financial year, the Commissioner will begin publishing the final reports of audits conducted on Commonwealth agencies.

4.2.2.6 Injunctions

Section 98 of the Privacy Act provides for the Privacy Commissioner (or another person) to seek an injunction from the courts to prevent or stop behaviour that is, or is potentially, contrary to the Privacy Act. To date this provision has not been used, but remains an important tool available to the Privacy Commissioner.

4.3 OFPC-proposed framework for considering potentially privacy intrusive policy or legislation

Key step	Things to consider, including:
Identify the problem	✓ Size & scope of the problem ✓ Likely longevity ✓ Implications in the Australian context
Identify the range of possible solutions	✓ The range of responses open to us ✓ Resource implications of these options ✓ Efficacy issues – which option/s will work best and not unduly affect people's lives?
Think carefully and clearly about the proposed solution	✓ What is the impact on privacy, and on whose privacy? ✓ Will the solution work and will it meet its target? ✓ What are the community's values here? ✓ Proportionality – is the measure proportional to the known risk?
What does the community think?	✓ What consultation or debate has occurred? ✓ What does it tell us?
Implementing the new powers	✓ Confer intrusive powers expressly in law (via an Act, not subordinate legislation) ✓ Legislation to state, expressly and objectively, the grounds on which the powers may be used ✓ Authority to exercise powers to rest at an appropriate level – to be expressly stated in legislation
Need to ensure transparency, accountability and reporting	✓ Make sure the community is kept informed about use of the powers ✓ Ensure a transparent and independent complaints-handling system, monitoring system and the powers of independent audit ✓ Include an independent and public assessment and reporting process for the operation of the measures ✓ Ensure reporting and oversight powers are commensurate with the intrusiveness of the measures ✓ Preferably spell out these arrangements in legislation, especially where the new powers are particularly intrusive
Review processes	✓ Parliamentary review of the measures after a fixed period – identify operational successes, as well as unintended or undesirable consequences ✓ Modify or remove powers as needed ✓ Include a 'sunset clause' – it is wise to pause and think again.