Speech to the Records and Information Management Professionals of Australasia

Wednesday 2 March 2011

By Commonwealth Ombudsman, Allan Asher

Introduction

I'd like to begin by acknowledging the traditional owners of this land on which we are meeting today, the Ngunnawal ("Nun-a-wall") people.

My thanks to the **Records and Information Management Professionals of Australasia** for two things: Firstly for the invitation to talk with you today be a part of RIMPA's professional development series—and also for the 'Disaster Preparation & Recovery Quick Reference Guide' that your association has published—I was particularly interested in this.

We have an office in Brisbane that was flooded and I was interested to some of the structured ways in which advance preparation can lead to much more cost effective outcomes for people.

But in addition to that I've just been in New Zealand meeting with the New Zealand Ombudsman and their office in Christchurch is in a multi-story office block. It's not one that collapsed in the earthquake but the stairwells collapsed and the staff were stuck on the eighth or ninth floor but because they have a disaster recovery program and they happen to have on staff, a fellow whose recreational activity was mountaineering, and they had ropes and axes and things in their emergency preparation area, he was able to knock out one of the windows and to lower each of the fourteen staff down to safety.

Quite spectacular, and it managed to get quite a bit of TV coverage but it meant that we'll have to change our job specifications for staff at the Ombudsman's office here.

Today I'd like to touch on the following themes:

- the need for a strategic approach to record keeping and information management–for government agencies to fully harness the contribution of information management professionals and understand that information management is about more than managing data
- the need to strive for improved openness and accessibility to information–to improve participation between government and community—and for fairness and transparency.

I'd like to then:

- briefly discuss the complementary work of the new Australian Information Commissioner, Freedom of Information Commissioner and Commonwealth Ombudsman in this area—and pose a few questions to consider
- examine in a bit more detail the Ombudsman's role, particularly how our complaint handling, investigation and *own motion* reports render a practical focus on the role of information management through a few case studies where the information systems have failed individuals, for one reason and another—and the consequences that arise
- draw attention to the difficulties of handling the amount of information that is generated

- conclude with two important lessons learnt from our work that should serve as a positive reinforcement of the importance of the work of information management professionals in government agencies.

In the late 1800s in Philadelphia there was a very successful businessman by the name of John Wanamaker.

Anyway, John Wanamaker is most often attributed with the famous advertising saying: *'Half the money I spend on advertising is wasted; the trouble is I don't know which half!'*

Maybe records management (in some ways) is a bit like this. At the time of keeping and storing information—at the time we record the data—we may not have a clear idea of what we'll want to retrieve later on, let alone every potential application. Its significance will not always be apparent.

So which bits (literally), do we want to keep? Do we just use a blanket approach and keep the lot? What are the implications of this approach? Or which half is the priority? as John Wanamaker said.

So there are necessarily many questions to consider like: What does my client require? Where and how do we keep it? For how long? How do we retrieve it? Who has access? How is it being made available to the public – if not – why not?

Do we have carefully considered and defendable reasons for the appropriate safeguarding or release of information to the community? This last question is one that agencies should already be tackling as they prepare to publish work practice manuals on 1 May.

We are dependent on an open system and that we need the free-flow of information to make the elements of our democracy work in a functional way.

These questions need to be considered at a strategic level—always with an eye to interests of the community and open government—and closely with information professionals who go to great pains to understand what information, and how much, needs to be recorded for possible use later on—and importantly, how it may be accessed and utilised.

The Wiki-leaks phenomenon shows the way vast amounts of information can be shifted around, and that the notion of security of information can be very doubtful.

I read that, of the American civil servants who have access to that level of clearance runs to some millions—and with this number of people with a high security clearance, it makes one wonder about the point of it all.

It has brought to the fore the question of access to information and what is in the public interest—this has seen another important aspect emerge to centre stage—the appropriateness of the information held.

Are we keeping information that should not be kept? Is it slanderous or salacious? Is it a comment on people's style or career ambitions, or contain personal and other inappropriate information? Should it be available to the community?

When considering the development of an effective information policy, issues we need consider include:

- What security measures are in place? Are they appropriate? Is there a coordinated approach? Are we sharing information and experiences? Do we have the capacity to keep pace with international developments and innovations in information management?
- What are the consequences of leaked information or of FOI requests or Public Interest Disclosures? Are we seeing these as a threat or opportunity? How should we prepare? How should we facilitate access to information?

No doubt there are many more. These are all valid questions that we should not be afraid to explore, as we strive to implement appropriate policies and importantly deliver more open government.

A change in the role of the Ombudsman: FOI and PIDs

This leads me onto a change in the role of the Commonwealth Ombudsman in the area of information management, with reforms to the *Freedom of Information Act* and anticipated Public Interest Disclosures (PIDs) legislation—or whistleblowing.

One of the resource pieces that I have bought with me today is a short article that we've written about whistleblower issues and it might be an interesting subject for this group to consider.

It's called 'Challenges in implementing a whistleblowing scheme', published in *Public Administration Today*, December 2010. This is also available on our website.

A new office came into effect on the 1st November last year—the Office of the Australian Information Commissioner (OAIC), and John McMillan has that separate statutory role. This is in advance of *new* information publication scheme requirements which come into effect on 1 May 2011.

It includes two new statutory officers: the Australian Information Commissioner and the Freedom of Information Commissioner, and incorporates the existing office of the Privacy Commissioner.

The aim of the OAIC in its simplest form–is to give the Australian community better access to information.

My role as it relates to freedom of information matters will be less—but I must stress my enthusiasm for this shift in the mindset of government administrators, toward greater openness, transparency and accountability.

The other passion of mine is for improved information accessibility–in the context of achieving greater social inclusion. Perhaps what I should refer to, is the problem of social exclusion. Because it's also the case that with the burgeoning amounts of data, agency after agency are putting material on websites or on other electronic platforms and are expecting people if they are going to have access to it at all, to have access to it electronically.

It remains the case that somewhere around half our population just don't have routine access to the technology that would allow that—or don't have the skills.

What starts of as a very positive thing for inclusion of individuals can have a negative impact. The digital divide is increasing.

People may be looking to efficiencies and economies of electronic data management, but failing to understand the importance of data to individuals whose lives can be badly affected by that.

There are those vulnerable individuals finding access difficult (or impossible) through illiteracy, homelessness or physical limitations. They may lack the equipment or the English skills or the cognitive capacity to engage properly in the electronic age.

Technology may well assist—but it can also hinder. Thought needs to go to the design of systems that facilitate accessibility.

When considering the accessibility to information by the community–whether it be an FOI request, the role of Wiki-leaks and like organisations, or more broadly the contribution that whistleblowers often make to a strong and robust democracy–the impact of Public Interest Disclosures (PIDs) is equally important to the discussion.

Legislation, that we anticipate will be considered by the Parliament in 2011, and if passed, will establish a new framework for handling the receipt, evaluation and investigation of PIDs, as well as the protections and rights of those who speak out about what they consider to be wrongdoing in public administration.

For a fuller exploration of the emerging challenges information professionals might need to consider, I'd encourage you to seek out the publication *Toward an Australian Government Information Policy—November 2010*, available on the website of the Office of the Australian Information Commissioner.

Role of the Ombudsman – examples of compromise

As a government 'watchdog' we are in the unique and privileged position—through our complaint handling role—to be able to identify common and re-occurring problems.

Case studies are illuminating and often bring to light a point of convergence. This is born out in the systemic issue of compromised tax file numbers which we recently investigated; more about this shortly.

In our investigations, case studies often point to incomplete, or a lack of information. We respond to particular issues, and these specific cases help to give us focus rather than use a blanket approach mentioned earlier.

We are regularly reminded of the practical importance of good record keeping and good information management. Why? Because it avoids problems—that later, will need to be fixed.

And we are well aware of the integral role that information managers play, in both safeguarding and educating others about the importance of effective, accountable and responsive management of information in the public interest.

Case studies are instructive; and shed light on where information systems have failed—we'll come to a few examples in a moment. A large part of our work means we are investigating government inefficiencies, inadequacies or failures in administrative processes. A person may have been poorly treated, or there may have been government systems or programs which have disadvantaged a number of people, or simply failed to comprehend all potential implications–however well planned.

Technology itself may have contributed to this. Within one agency there may be different systems being used—or they may not be connected. Information may not be cross-referenced, so there is poor access. Disparate storage areas may not be linked.

Some of our suggestions and recommendations have included:

- that copies of reports are readily retrievable
- provision of adequate documentary record of assessment processes
- undertaking review of record keeping practices and modify them where appropriate
- documenting reasons for decisions
- clarity on the appropriate record keeping needs to be given to staff
- data needs to be able to be tracked, extracted and measured.

The list goes on and on. Agencies are usually happy to receive recommendations, and invariably set about making changes to improve systems.

Cropping up in Ombudsman investigation reports, over and over again are phrases, statements and recommendations about information management. Here are a few:

Centrelink

1. This is a brief extract from a Centrelink report last year about circumstances leading to a fraud conviction—***Centrelink and Commonwealth Director of Public Prosecutions: Review of circumstances leading to a fraud conviction—May 2010 (07/2010)*.**

> *'There was no indication from the documents provided that follow up action had been taken by Centrelink ... The electronic records did not contain complete details of the documentation submitted'.*

The obvious lack of record keeping is commonly highlighted in our investigation reports—this business of documentation. I've seen quotes from customers saying something like: "I've already shown you my documents once—why do I have to bring them in again?"

Customs

And another highlighted through our investigation into the strong coercive powers exercised by Customs officers—***Australian Customs and Border protection Service: Administration of Coercive powers in passenger processing—Nov. 2010 (15/2010)*.**

They have the authority to question passengers and examine goods such as diaries, mobile phones, cameras and computers. They can copy documents and retain a person's possessions for a period. So strong checks and balances are called for; and proper records need to be maintained. We found that there were gaps between policy and practice in record keeping—that the checks and balance were not always as good as they should be.

Sometimes there are poor explanations given as to why goods are being taken away; why certain questions are being asked; and then also the difficulties for individuals in recovering devices.

I wonder how you would feel and what you'd do if, like me, your itinerary information, contact information, even passwords for credit cards and the like, might be stored on an electronic device that's taken away from you when you land in a foreign country—and you might not get it bacvk for a week or two.

So we say that there needs to close scrutiny and auditing on how coercive powers like this are used.

This was one of the report's recommendations to the Customs and Border Protection Service:

> *'Customs should conduct a regular audit to check whether records of the exercise of the coercive powers are being kept in line with Customs internal guidelines. The findings of that audit should form the basis of further staff training or mentoring'.*

Here are some more detailed examples with case studies that highlight the 'real' impact on individuals.

<u>Child Support Agency-CSA</u>

In November we released a report on the Child Support Agency's 'write only' policy. ***(Department of Human Services, Child Support Agency: Unreasonable customer conduct and 'Write only' policy—Nov 2010 (14/2010), Case study on page 21).***

This is a strategy for managing a customer's unreasonable conduct–it means that case officers will only engage with individuals in writing, not over the telephone or face-to-face. The header for our media release read: "Difficult behaviour shouldn't mean inadequate service".

One can understand that parents who are separating and sorting out custody and financial arrangements can be very unsettled emotionally—and their conduct can become unreasonable.

There is also the need to protect CSA staff from possible harm; and, they can reasonably expect to be treated with civility in their work. The report casts light on communication and record keeping problems.

I should use one of the case studies from the report to demonstrate some of the difficulties which can arise from inadequate record keeping:

<u>Case study - Mr J</u>

- Mr J had a history of using offensive language and made inappropriate and threatening comments to the CSA.
- In early 2003, the CSA decided to restrict Mr J 'write only' contact.
- The CSA could not locate the submission in this regard, nor could it find reasons for the decision or a copy of the letter to the customer advising him of the decision.
- The only record of the decision the CSA could produce was a computer notation stating that the CSA's General Manager had signed a letter advising Mr J that he was 'write only' customer.

- This appeared to be the second time that the CSA had made Mr J a ‘write only’ customer.
- However, the CSA could not locate any records about its earlier decision to remove the ‘write only’ status or the decision to reinstate it.
- Sketchy computer notes made afterwards suggested that the CSA reinstated Mr J’s ‘write only’ status when it was unable to reach an agreement with him about the content and desired outcomes of a proposed meeting.
- This tends to suggest that the CSA imposed the restriction when it reached the point of exasperation with Mr J.
- In 2006, Mr J requested that he be allowed to contact the CSA via telephone.
- The CSA did not consider his request and made a note on his record that he was ‘unable to change his status as a write only client’.
- In 2008, the CSA advised Mr J that he would not be offered the opportunity to contact it via telephone ‘unless he puts in writing the reasons why it would assist him and he commits to stop verbally abusing CSA staff’.

It is plain to see that Mr J’s difficulties largely stemmed from record mismanagement.

So the consequences of poor information storage and management and communication are all around us—and a good part of our work relates to just that—wether it’s about Tax file numbers or Centrelink ‘write only’ policies or the general descriptions used by government agencies on how decisions are made or how to access information.

Your work—the work of information management professionals—is crucial to the performance of agencies. The consequences of poor information management are all too often evident in the case studies we examine.

So it’s not just numbers, or data or statistics—there are real repercussions. We are talking about real impacts to people’s lives.

ATO

The second example comes from an ‘own motion’ investigation into the Australian Tax Office. In September of last year we released a report on the Tax Office and Compromised Tax File Numbers—***Australian Taxation Office: Resolving Tax File Number Compromise—Sept. 2010 (12/2010)*****.**

The report examined case studies where taxpayer’s TFNs had been compromised or incorrectly linked by the ATO to another person’s TFN. As you can imagine, when this unique identifying number is compromised the impacts on a taxpayer can be significant. It can cause delayed refunds and payments, debts being incorrectly attributed to the taxpayer or problems with other agencies like Centrelink, where information is exchanged.

Here is a case study described in that report; where the ATO’s computer system somehow showed that more than one TFN existed for one taxpayer:

- Mrs D’s difficulties began when the ATO wrongly determined that she had two TFNs.
- In fact, Mrs D only had one TFN and the other number belonged to another taxpayer.

- The error meant that Mrs D had income incorrectly attributed to her.
- This was upsetting and difficult to resolve, not least because English is not her first language.
- Mrs D complained in writing but nothing happened.
- Finally, after two years and an Ombudsman investigation, the TFN confusion was sorted out.

So the problem lay in the retrieval of the data. And there are many other similar cases. In this case the Tax File Number is used as the primary identifier in the administration of the taxation system—so it is clear that good information management is critical.

TFN as Super identifier

While on the subject of Tax File Numbers, submissions recently closed into a Treasury review considering the use of TFNs as an identifier for superannuation. The suggestion being that it may offer practical benefits in the consolidation and management of superannuation fund members' accounts.

In our submission, we have restated the need to implement effective procedures and systems with data management to ensure:

- the integrity of the identity matching process including establishment of an identity matching standard
- safeguards against instances of TFN compromise through fraud, accidental disclosure or operator error.

Alvarez report (Ombudsman 2005)

I suppose one of the all-time low points in records management in Australia would be the **Vivian Alvarez Solon** case—when she was unlawfully removed (by the then DIMIA – now DIAC) from Australia to the Philippines in 2001 after an immigration officer wrongly presumed she was a sex slave and an illegal immigrant.

There was poor record keeping, poor inquires, and a great lackness which led to that very severe result.

In our report, ***Inquiry into the Circumstances of the Vivian Alvarez Matter (03/2005)***, we observed:

> *'The Inquiry's investigation brought to light major flaws in DIMIA's case management. The flaws extend from poor record keeping to completely inadequate accountability processes ... A series of failures to manage Vivian's case effectively was an important contributor to the failure to identify her...*
>
> *The biggest deficiency associated with the Alvarez files is the lack of adequate records. Vital information and crucial decisions were not recorded. There is evidence of irregularities in file dates. Original notes were lost 'in the system', without copies having been made. Case details that were inaccurate and potentially misleading were forwarded to senior staff.*
>
> *DIMIA staff told the Inquiry that in some situations they deliberately left their actions unrecorded...*

> [the report went on to say] *'There is no record of an actual decision to remove Vivian—if one was made'.*
>
> [there is also an instruction which] *'requires that a compulsory checklist be completed ... (but) there is no evidence that such a checklist was ever completed ... Within DIMIA there is a serious problem with the training of compliance officers in ... the use of IT systems and databases. This problem undoubtedly contributed to the failure to identify Vivian and requires urgent redress'.*

Once again, the need for good records and effective data management can be critical in establishing someone's correct identify.

More recently there were issues around what information was available with the refugee ship that broke up on Christmas Island late last year. It is still too early to see what is going to happen from that, but information management is going to be an important part of that joint Parliamentary Committee that was established just today.

Ten Principles for good public administration

Our office prepared a series of reports from 2005 to 2007, out of the investigation of some 247 cases of immigration detention. Administrative information management errors were highlighted, and drawing from those examples we identified ten principles of good administration, to be found in our report *Lessons for public administration–Ombudsman investigation for referred immigration cases–11/2007*. I've brought along copies of our *Factsheet 5: Ten principles for good administration* which summarise these lessons.

They are particularly relevant to decision making that can have adverse impacts on the rights, liabilities and entitlements of members of the public.

There are two of these principles I would particularly draw your attention to, that dealt specifically with records management—namely no's **1** and **4**.

The *first* principle is:
<u>Maintain accurate, comprehensive and accessible records.</u>
An error as simple as misspelling someone's name, misstating their date of birth or misfiling their application for a benefit can have serious consequences.

- A mistaken record can result in a person being wrongly detained, incurring a penalty, losing or being denied a benefit, or having legal proceedings initiated against them.
- Agencies must ensure that a strong agency culture supports good record management as essential to high quality decision making.
- Administrative systems must accurately record client details.
- Staff should be well trained and supported in good record management practices, with clear, accessible and current policy guidance.
- Quality assurance mechanisms should apply to all stages of records management.

The *fourth* principle is:
Heed the limitations of information technology systems.
We trust in technology, but automated systems are no better or more reliable than the data entered on them.

- Staff must not assume, for example, that information they find on their system about a person's status is always correct, or that conflicting information received from a person is false or dubious—that if the 'machine said it, it must be right'. Too often people assign higher levels of veracity to things that are recorded than they ought.
- It is always possible that information on the system is incorrect, was wrongly entered, or was not retrieved fully because the wrong search parameters were used.
- Equally, a design or programming error can taint decisions that are based on the information in the system.

Agencies should ensure that IT systems reflect their business processes and the legislation they administer, and that they support accurate decision making.

- Where there are different systems for different business processes, they should be properly integrated.
- Staff training must emphasise the need for caution when entering or retrieving data and basing decisions on the data in a system.

In my experience once errors of this type occur, apart from the consequences for individuals, the actual costs to agencies can be huge as well—the costs of going back and redoing sometimes months or years of input; of having to bring in extensive and expensive external audit.

So as a clever risk management process any information system in my view really should invest in something of that character.

I've used just a few examples—but as I say a good part of all of the work we do somehow comes down to adequacy, accuracy, timeliness or availability of information.

All too often our concerns will be about how well the department or agency handles its information. It is a recurring theme.

Good information management demands accuracy and accessibility. It means using properly integrated Information Technology systems, with caution and an eye to correctness of data. It must also be underpinned by a demonstrable commitment to open government and facilitating effective engagement with the community.

I hope that this organisation will continue the work that it is doing in ensuring that things are improving on this front.

I wish you well on your journey toward better practice information management.

Thank you for listening to me and thank you for your time.

***