

Effective Information Management – the Keystone of Good Government

*Prof John McMillan, Australian Information Commissioner
Presentation to the 10th World Conference of the International Ombudsman Institute,
Wellington, New Zealand, 15 November 2012*

I will bookend today's presentation with two incidents that received wide international publicity in the last week.

One incident was the resignation in Great Britain, after only 54 days in the job, of the Director-General of the BBC, George Entwistle. He resigned after admitting he had failed to check the evidence before allowing a BBC program to be televised which wrongly named Lord McAlpine, a senior Conservative member of parliament, as a sexual predator.

The other episode was the re-election of US President Barak Obama. Commentators noted that a key element in his re-election was the expertise of his support staff in applying to a Presidential campaign the same data analytics that are successfully applied to supermarket sales promotions.¹ Their data-driven metric capacity to disaggregate the voting community into an infinite range of demographic groups gave the Obama campaign an edge in fundraising, targeting campaign messages, designing TV promotions, selecting campaign methods, deciding priorities, finding lost voters, predicting voter response and connecting the candidate with all segments of the community.

A different but related message can be drawn from both stories: defective information management can have disastrous and unjust consequences, while effective information management can harvest enormous value from a rich resource.

Those messages are captured in the title of my paper: 'effective information management is the keystone of good government'. Every decision, every action, every policy, every program administered by government uses information. The quality of all government decisions and actions is conditioned by how wisely and appropriately information is collected, stored, managed, used and disclosed. The information that underpins government administration must be accurate, complete, discoverable, accessible and useable. As noted recently by the Australian National Audit Office in a report on *Records Management in the Australian Public Service*: 'A key element of sound public administration and accountability is adequate record keeping or documentation of the business of government'.²

I will illustrate those points with examples drawn from four areas of activity in my former role as Commonwealth Ombudsman (2003-10) and my current role of Information Commissioner (2010-).

¹ Eg, Tim Murphy, 'Under the Hood of Team Obama's Tech Operation',

<http://www.motherjones.com/politics/2012/11/inside-obama-campaign-tech-operation>

² ANAO, *Records Management in the Australian Public Service*, ANAO Audit Report No 53 2011-12.

Ombudsman reflections on record keeping

Every Ombudsman can give examples drawn from investigations of agency maladministration that occurred through defective record keeping. The most telling example in my work was a large scale systemic investigation of 247 cases of immigration detention that led to eight published reports.³ Legal and factual errors were found in nearly all 247 cases, including the immigration detention of 26 Australian citizens, the wrongful detention of 10 children and wrongful detention for as long as 6½ years in one case.

In a concluding report entitled *Lessons for Public Administration*, the first of ten lessons was 'Maintain accurate, comprehensive and accessible records'.⁴ Very simply, inexcusable record keeping errors and poor information management was a frequent cause of wrongful detention and loss of liberty. Great injury stemmed from record keeping errors as trifling as misspelling a person's name, misrecording their date of birth, losing or misfiling documents and not cross-referencing related files.

The same lesson can be seen in other areas of administration. An inaccurate record, a misfiled document and sloppy records management can result in a person losing an income support benefit, being refused a business assistance grant, incurring a penalty for alleged failure to lodge a return, being wrongly prosecuted, receiving conflicting demands from a government agency, or having sensitive personal information publicly released.

There are similarly alarming examples from other Australian Ombudsman reports of the damage caused by record keeping errors. An example from the NSW Ombudsman was a report in 2006 that found instances in which DNA computer records were inaccurate.⁵ In one case a DNA sample was placed on the wrong file; in another the files of two people with similar names were combined. A report last year from the Victorian Ombudsman concluded that poor record keeping by private sector organisations that administered a government insurance compensation scheme lay behind a 27% increase in complaints to the Ombudsman over three years.⁶ Sloppy record keeping led to delayed insurance payments, privacy breaches, poor decision making and manipulation of the scheme by the private sector administrators.

It is equally important in Ombudsman work to draw attention to good record keeping that supports an agency's claim that it acted properly. An example from my work was a large scale investigation into allegations that the Defence Department was forewarned of a safety

³ See J McMillan, 'Lessons for Public Administration: The Ombudsman Investigation of Referred Immigration Cases' (2007) *Public Administration Today* 36

⁴ Commonwealth Ombudsman, *Lessons for Public Administration*, Report No 11 of 2007

⁵ NSW Ombudsman, *DNA sampling and other forensic procedures conducted on suspects and volunteers under the Crimes (Forensic Procedures) Act 2000* (Oct 2006) at vi.

⁶ Victorian Ombudsman, *Investigation into Record Keeping Failures by WorkSafe Agents* (May 2011).

risk that caused a fire and fatalities on a naval destroyer.⁷ Everyday Defence records that had been properly prepared and maintained many years earlier, such as running sheets and file notes, enabled me to conclude that the Defence Department had not been forewarned of the fire risk and that mysterious documents to the contrary that were purportedly Defence records in fact lacked authenticity and credibility. I concluded that 'It is not always clear at the time a record is created how important it may be in the future. It is inevitable that some administrative decisions and actions will later be questioned, though which ones is never clear at the time. Good record keeping is ultimately a time saving rather than a time wasting activity.'⁸

Information Commissioner reflections on information management

Turning now to my Information Commissioner role, the Office of the Australian Information Commissioner (OAIC) has responsibility for three areas that all require a strong focus on government information management – freedom of information, privacy protection and information policy advice to government. The joinder of those three areas in a single office itself conveys an important message. Integrated information management must be seen as a key responsibility in all areas of government.

It is axiomatic that the smooth operation of the *Freedom of Information Act 1982* depends on the capacity of agencies quickly to locate documents that fall within the scope of a person's access request. This is a constant theme in our work when reviewing agency FOI access refusal decisions and investigating complaints against agency FOI administration.

A comparison of two large agencies bears this out. The Defence Department is generally regarded as being one of the best performing agencies at present in FOI administration. Although the Department is the largest public sector employer in Australia, it boasts compliance with FOI time limits in handling 100% of FOI requests. This success rests on Defence knowing at which of its numerous offices and bases across Australia a record will be found, assigning responsibility for locating a record and making the FOI decision to officials in both the central and the regional offices, accrediting those officials through an internal course on FOI administration, and moving those functions from the legal section of Defence to a section staffed by information professionals.

The OAIC was, on the other hand, critical of FOI administration in the Department of Immigration in a recent report stemming from an own motion investigation.⁹ The Department receives the highest number of FOI requests of all Australian Government

⁷ Commonwealth Ombudsman, *Department of Defence: Allegations Concerning the HMAS Westralia Fire*, Report No 3/2008.

⁸ Commonwealth Ombudsman, *E Bulletin No 2* (2008)
<http://www.ombudsman.gov.au/pages/publications-and-media/e-bulletins/e-bulletin-02.php>

⁹ Australian Information Commissioner, *Processing of non-routine FOI requests by the Department of Immigration and Citizenship*, Report No OM12/00001 (Sept 2012).

agencies. Over 96% of its requests are for personal information, and it complies with FOI time limits in 88% of those cases, which are mostly handled in regional offices. However, the Department has an unsatisfactory record in handling complex requests for non-personal information from journalists and members of parliament. Less than 20% are handled within the statutory timeframes, and the delays stretch into the hundreds of days. The need for improved records management practices was a strong theme in the report.

The second responsibility of the OAIC is to administer the *Privacy Act 1988*. The core focus of that role is to ensure that government and industry observe Information Privacy Principles in the way they handle personal information. However, that brief description can understate the growing importance of privacy management in government planning and administration.

Much of the information held by government can be traced to an individual – a name, an address, a telephone number or some other personal identifier. Increasingly, public acceptance of new government programs can depend on reassuring the community that personal information will be securely and properly managed. New programs on which my office was consulted by agencies in the past year include a new ehealth records system, passenger body scanning, student identifiers, cloud computing, smart metering, superannuation reform, service delivery restructuring, cybercrime, financial transactions reporting, identity management, personal properties security, and media regulation.

As those examples indicate, government does not have the practical option of managing personal information by segregating it and placing it in a locked and impenetrable storage. The value of all information, including personal information, resides in the ability of agencies to use it – to collect it, analyse it, rearrange it, link it, convert it and share it with others. Personal information, as a World Economic Forum report in 2011 stated, is ‘the new oil’, a new economic asset class.¹⁰

The challenge for government is to reassure the community that this personal information is an active data resource that can be securely managed. Technology provides the means for doing so, but technology also provides the risk of calamitous failure. Ten years ago our greatest organisational fear was that a staff member in the mail room would put the wrong letter in an envelope, or would lose a briefcase containing a personal file. Now, the greatest fear in many organisations is that a staff member will lose a USB stick or CD rom that contains sensitive personal information about tens of thousands of clients, or will wrongly divulge their password that provides entry to the entire agency data base, or that a hacker will penetrate an inadequate security perimeter.

These fears are illustrated by some of the own motion investigations that my office has recently conducted. They include:

¹⁰ World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (2011).

- the investigation of a Telstra mailout that sent 220,000 letters with personal information to the wrong addresses
- the inadvertent collection by Google Street View cameras of unsecured wi-fi data from personal wireless networks
- Vodafone's failure to implement effective password security measures to protect the personal information it held on 4 million customers
- a cyber attack on the Sony Playstation network that exposed the personal files of 77 million customers.

The third responsibility of the OAIC is to promote information policy in government. Our particular focus is upon advancing open government through proactive information release and open data. The phrase 'government information' has been replaced by a more evocative phrase, 'public sector information' or PSI.

Information is a valuable resource that underpins all the public functions that government discharges. Public sector information is an equally valuable resource outside government. People and businesses use PSI to evaluate government performance, provide ideas and commentary to government, work in partnership with government agencies in delivering services, conduct research, plan business ventures, and drive innovation. This protean concept is neatly captured in a new objects clause in the federal Freedom of Information Act, declaring that 'information held by the Government is to be managed for public purposes, and is a national resource' (s 3(3)).

The best illustration of that point is that each of us, every day, more than once, and in different ways, relies on the same free source of government information – weather forecasts – to plan what we are doing. Yet in fact that process of providing weather information to the public is an immensely complex process that raises nearly every important information management issue – collection, analysis, verification, security, publication, discoverability, accessibility, re-use and potential liability for inaccuracy or misinterpretation.

The information interface between government and the community can be similarly complex in managing other government data holdings. The principal strategy for addressing this complexity has been the development of guiding principles and standards for information management. I will give two examples.

One is a set of *Principles on Open Public Sector Information* that the OAIC published two years ago.¹¹ The vitality of Principle No 1 – that open access must be the default position – depends upon seven other principles, stipulating that agencies adopt information governance arrangements, develop a register of information assets, make a senior officer responsible for information management, publish information on open licensing terms, make PSI discoverable through attachment of appropriate metadata, consult the public as

¹¹ OAIC, http://www.oaic.gov.au/publications/agency_resources/principles_on_psi_short.html

to what PSI is of use or interest to them, and establish a transparent enquiry and complaints framework to capture public feedback about agency publication and access decisions.

A second set of standards is the *Digital Continuity Principles* recently published by the National Archives of Australia.¹² The aim is to move all federal government agencies to the default position of digital records management.

Partly this is a practical and resource initiative. Federal Government agencies currently store nearly 1400 shelf kilometres of paper records, growing by over 100 kilometres per year, at an estimated annual cost of more than \$220M. Partly too it is an information management challenge. As the new policy explains, digital continuity is all about using information so that you can –

- find information when you need it
- open it when you need it
- work with it in the way you need to
- understand what it is and what it is about
- trust that it is what it says it is, and
- keep it for as long as required but no longer.

That is the new record keeping challenge in a digital age of complex government.

Conclusion

I will close with five lessons for Ombudsman and Information Commissioners.

First, we must use the opportunities that our work provides to draw attention to record keeping and information management issues. We are in the unique position that we examine administrative practices across all of government. We are uniquely placed to identify and publicise instances that display bad and good practice. Individual case studies can be a lesson to all of government. To the extent possible, we should make record keeping and information management a sub-theme of all that we investigate.

Secondly, our message to government can be more practical and sophisticated than ‘good record keeping is essential’. Beyond our walls there is a profession that specialises in record keeping and information management. Excellent guidance is available in numerous codes, standards, web resources, education courses and consultancy services. We should use those standards as a benchmark for gauging whether agency practices are deficient. We should ask pointed questions of agencies and require them where necessary to rehabilitate their accustomed practices.

Thirdly, we should establish active working links with other agencies that have an information policy function. To give one example, both as Ombudsman and as Information

¹² NAA, <http://www.naa.gov.au/records-management/agency/digital/digital-continuity/index.aspx>

Commissioner I found a great ally in the Archives Office. It has developed many of the record keeping standards that agencies are expected to observe. My office can highlight telling examples of the damage caused by a breach of those standards.

Fourthly, we should promote regular audits of agency information management. While complaint investigations can pick up random instances of bad and good practice, information management is an issue in the 99.999% of decisions that we never see. Case file auditing can be more effective in identifying systemic problems. Our offices can undertake those audits, but a better strategy will usually be that an agency appoints an independent expert to do the audit and publish the audit report.

Fifthly, Ombudsman and Information Commissioners must lead by example. Effective information management is as vital to the success and reputation of our work as that of other agencies. We cannot credibly criticise the defects of other agencies if we are no better. An example of the practical steps that we can personally take in our own offices is to check, in any hard copy file that crosses our desk, whether our office staff are folio numbering documents and maintaining files in good order. Looking to the future we should be moving our offices to a digital and paper-free environment. There should also be an internal training program in information management that all staff, including the head of agency, is required to undertake.



Australian Government

Office of the Australian Information Commissioner



Protecting information rights — advancing information
policy



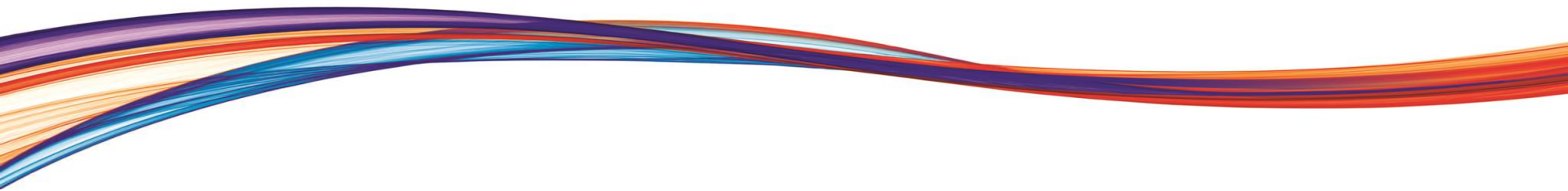
Australian Government

Office of the Australian Information Commissioner

Effective information management – the keystone of good government

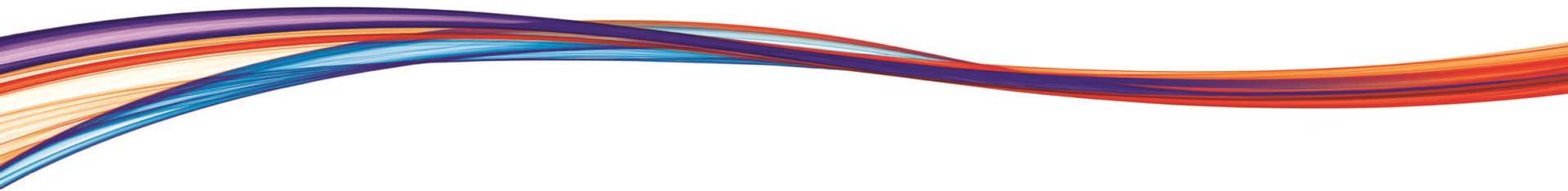
John McMillan

Australian Information Commissioner

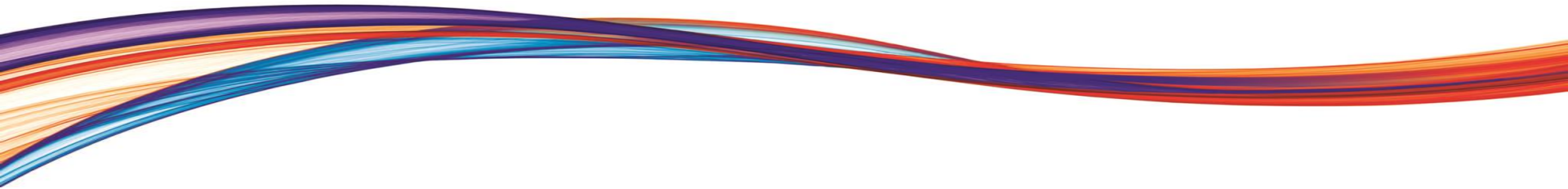


Record keeping case studies

- Ombudsman investigations
 - *Lessons for Public Administration: Lesson 1: 'Maintain accurate, comprehensive and accessible records'*
- FOI handling
- Protection of personal information
- Promoting an open government culture
 - *Principles on Open Public Sector Information*
 - *Digital Continuity Principles*



Ombudsman/Commission challenges

- Highlight good and bad practice in information management by agencies
 - Require agencies to apply professional information management standards
 - Work with agencies that are information specialists
 - Promote regular audits of information management in agencies
 - Exemplify best practice in information management
- 



Australian Government

Office of the Australian Information Commissioner

Questions?

Protecting information rights – advancing information policy

www.oaic.gov.au