Hazard reduction in privacy management: ongoing issues in the NSW Fire Brigades

Anne Pickles, Information Coordinator, NSW Fire Brigades

Abstract

The *Privacy and Personal Information Protection Act 1998* came into force in NSW in July 2000. The NSW Fire Brigades developed and implemented a Privacy Management Plan to ensure that it complied with the law. Through this process, the NSW Fire Brigades addressed all the obvious issues relating to its major collections of personal information. This paper will look at some of the privacy issues that have arisen in the NSW Fire Brigades since the implementation of the Privacy Management Plan. Some issues arise from changes in operations or technology, such as the introduction of employee self service, new community risk management programs, or the development of fire station Internet sites. Others arise from changes to the environment in which the NSW Fire Brigades operates, such as increased security risks. Growing awareness of privacy in the NSW Fire Brigades has contributed to the improvement of information management processes and systems and is reducing the risk of negative outcomes in employee relations and services to the community.

Introduction

The *Privacy and Personal Information Protection Act 1998* (the PPIPA) came into force in NSW in July 2000. This act establishes a number of information protection principles for the management of personal information by NSW government agencies. It is modelled on the Commonwealth *Privacy Act 1988,* which covers Federal government agencies and the private sector. A number of other Australian states have also introduced or are considering privacy legislation.

As a NSW Government department, the NSW Fire Brigades (NSWFB) is subject to the PPIPA. The NSWFB provides fire prevention, protection, mitigation and suppression services to major metropolitan areas, regional centres and rural towns in NSW. The NSWFB also provides rescue services and is responsible for managing hazardous materials incidents throughout NSW. To provide these services, the NSWFB maintains a network of 338 fire stations and employs some 3200 full time firefighters, 3200 part time firefighters and 330 support staff, and has 4300 volunteer Community Fire Unit members. In 2002/03 the NSWFB attended over 128 000 incidents.

What is personal information?

Under the PPIPA, personal information is any information that relates to an identifiable person. This definition covers not only paper records, but also such things as genetic material, electronic records, audio or video recordings, photographs and biometric information such as fingerprints.

Names, addresses, phone numbers, tax file numbers, bank account numbers, vehicle registration numbers and information or opinions on a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual activities are all personal information.

The person's name need not be included in the information to make it personal information - if the person can be reasonably identified from the information, then it is personal information. For example, the information that a fire occurred at a particular address at a particular time can be considered to be personal information as it is generally fairly easy to identify the occupant or owner given this information.

The Information Protection Principles

Twelve Information Protection Principles relating to the collection, use and disclosure of personal information form the basis of the PPIPA. The following brief summary is taken from Privacy NSW's website(1):

Collection

1. **Lawful** - when an agency collects your personal information, the information must be collected for a lawful purpose. It must also be directly related to the agency's activities and necessary for that purpose.

2. **Direct** - your information must be collected directly from you, unless you have given your consent otherwise. Parents and guardians can give consent for minors.

3. **Open** - you must be informed that the information is being collected, why it is being collected and who will be storing and using it. The agency should also tell you how you can see and correct this information.

4. **Relevant** - the agency must ensure that the information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

5. **Secure** - your information must be stored securely, not kept for any longer than necessary, and disposed of appropriately. It should be protected from unauthorised use or disclosure.

Access

6. **Transparent** - the agency must provide you with enough details about what personal information they are storing, why they are storing it and what rights you have to access it.

7. **Accessible** - the agency must allow you to access your personal information without unreasonable delay and expense.

8. **Correct** - the agency must allow you to update, correct or amend your personal information where necessary.

Use

9. **Accurate** - agencies must make sure that your information is accurate before using it.

10. **Limited** - agencies can only use your information for the purpose for which it was collected, for a directly related purpose, or for a purpose to which you have given your consent. It can also be used without your consent in order to deal with a serious and imminent threat to any person's health or safety.

Disclosure

11. **Restricted** - the agency can only disclose your information with your consent or if you were told at the time they collected it from you that they would do so. The agency can also disclose your information if it is for a related purpose and they don't think that you would object. Your information can also be used without your consent in order to deal with a serious and imminent threat to any person's health or safety.

12. **Safeguarded** - the agency cannot disclose your sensitive personal information without your consent, for example information about your ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without your consent in order to deal with a serious and imminent threat to any person's health and safety.

Privacy Management Plan

When the PPIPA was introduced in 2000, the NSWFB conducted an audit of its personal information assets, undertook a risk assessment of those assets against the requirements of the PPIPA, and developed a Privacy Management Plan for dealing with privacy issues. An audit of the outcomes of the Privacy Management Plan was commissioned in 2001 and it found that the majority of issues raised in the plan had been dealt with. I have dealt with this process in previously published papers [(2)(3)(4)]. The intent of this paper is to discuss privacy issues that have arisen since the initial introduction of privacy management in the NSWFB and how they have been integrated into information management practices. As with bushfire prevention, a risk management approach and appropriate hazard reduction measures reduce the likelihood of major incidents in the future.

My involvement with these issues stems from the fact that since the adoption of the Privacy Management Plan I have been the NSWFB's Privacy Contact Officer. Each NSW Government agency has a Privacy Contact Officer who is the first point of enquiry for staff, members of the public and other government agencies on privacy issues. The role of Privacy Contact Officer is one part of my duties as the NSWFB's Information Coordinator, in which position I am also involved in a wide range of knowledge management issues. I, in common with most NSW Government Privacy

Contact Officers, have no legal training, just an informed knowledge of the PPIPA and its application to the NSWFB. Nothing in this paper should be regarded as legal advice.

Images of the dead and injured

This issue first arose not as a privacy issue, but as an occupational health and safety complaint. The complaint was that firefighters at a station were keeping albums of photos of dead and injured people at rescue incidents and that this practice, and the way the albums were used by some firefighters, were causing the complainant distress. Investigation revealed that such images were being kept in a number of places in the NSWFB and that their taking and use was not being appropriately managed. In some cases, they had ended up on fire station Internet sites.

This obviously breached a number of privacy principles: the photos were in most cases taken without the knowledge or consent of the victims or their families, they were not being kept securely, and they were being inappropriately used and disclosed. As Privacy Contact Officer, I convened a meeting of the relevant managers to discuss the whole issue of taking and using such images.

When discussing privacy issues, I find it useful to go right back to first principles and begin with the *purpose* for which the information is collected and used. The question I put to the managers was, therefore, do we need to take and use these images at all? Cameras are so ubiquitous these days, that many people do not think before taking a photo or video, it just seems part of normal activities. Indeed, we encourage our firefighters to take pictures of incidents (when it is safe and convenient to the Incident Controller) for use for internal communications and training and for supply to the media. However, images of the victims of incidents are highly sensitive and taking and using such images can cause acute distress to the victims and their friends and relations, as well as to other viewers of the images.

After discussion, it was decided that, except where the NSWFB's Fire Investigation and Research Unit needed to collect images as evidence at a fire, there was no reason for NSWFB staff to be taking pictures of dead or injured people, not even for training except in exceptional circumstances. The discussion also revealed that there were some very useful management practices in place that could be extended to cover the whole organisation. The Fire Investigation and Research Unit pointed out that there was also an issue with getting these images developed: the developer had to be aware of the types of image involved and had to treat them as secure. For this reason Fire Investigation and Research has a contract with a single film processor who has agreed to these terms.

The outcome was a NSWFB policy on photographs and videos of dead or injured people. A copy of this policy is given in appendix A of this paper.

Workplace security

Once the issue of management of images of victims of incidents was settled, another issue arose on the management of images taken by security cameras at NSWFB workplaces. The use of security cameras in workplaces is becoming more common

and there are a number of sensitive NSWFB premises that have such systems in place. The NSW Government has a *Code of practice for the use of overt video surveillance in the workplace*(5) which gives some guidance on the issues, but it was issued before the introduction of the PPIPA. One issue is the rate of change in the technology. The NSW Government's code is several years old and assumes the use of videotape, while most modern systems take digital images. They may also only take images when something changes in their field of view, making requirements to inform staff of the length of time images are kept difficult, as it will vary with the amount of activity at the site.

Privacy issues related to overt video surveillance include: making sure that the surveillance is overt and not covert and therefore legal; informing employees and visitors to NSWFB sites that video surveillance is taking place; informing employees of their rights to access images of themselves; and informing employees of what the NSWFB will do with the information and when it may be disclosed to other agencies.

The NSW Government has now produced an exposure draft of a new Workplace Surveillance Bill 2004(6). The current NSW *Workplace Video Surveillance Act 1998* covers only covert video surveillance. The new bill covers both overt and covert surveillance and covers not only video surveillance but also surveillance of email, Internet access and activities on computer applications. This means that NSW Government agencies will have to comply with both the PPIPA and the new act in relation to all these activities.

In the current security environment, the NSWFB is also introducing or upgrading other security systems, such as security passes for access to NSWFB premises, identity and access management in NSWFB computer systems and incident ground management. In all cases where the information collected by the system can be related to an individual, the PPIPA will apply.

Internet sites

The NSWFB has recently redeveloped its website (www.fire.nsw.gov.au) and this was seen as an opportunity to document some of the privacy management practices required for publishing information on the Internet.

Information published on the Internet on an unrestricted site is available to anyone in the world with an Internet connection. It is therefore important to ensure that the information on the site does not breach any relevant laws. To ensure that users of our website are informed about the information, such as web logs and session cookies, that we will collect about them when they use our website, our website now includes a privacy policy(7). This policy says what we will do with the information and informs users how they can contact us if they have any queries. At this stage, not much information is collected; most of it is for statistical purposes. However, our next permanent firefighter recruitment campaign will require applicants to submit their applications electronically over a secure website. Privacy management requirements are built into the contract with the recruitment agency. In the long term, we will be looking at electronic delivery of services through our website.

The next stage of our Internet redevelopment is to improve our management of fire station websites. A number of fire station crews have created their own unofficial websites, with varying degrees of sophistication. We are now working to bring all station sites under our main Internet site, with appropriate policies and procedures in place to ensure that these sites do not breach the Information Protection Principles. These will cover such things as posting the names and photographs of firefighters on the site, how much detail it is appropriate to give about incidents, use of images, and whether guestbooks or bulletin boards are permitted.

Family history

The history of the NSWFB goes back to the founding of the Metropolitan Fire Brigade in Sydney in 1884. Since that time thousands of people have been employed by the organisation. A firefighter makes an interesting ancestor, so it is not surprising that the NSWFB gets regular family history enquiries. The NSWFB's Records Section assists with these, subject to resource availability.

If the person has been dead for more than 30 years, there is no problem as the information is then exempt from the PPIPA. However, if the person is still alive, or if we have no evidence that they are dead, it becomes more difficult. One area of difficulty is to decide whether information contained in some NSWFB or NSW Government publications can be regarded as being in a 'publicly available publication' in which case it would be exempt under section 4 (3) (b) of the PPIPA. Details of appointments, promotions, resignations and retirements are regularly published in this type of publication. Privacy NSW has identified that this as an issue in the current review of the PPIPA[(8)], as, for instance, publication of a birth notice in a newspaper could be regarded as making that person's date of birth exempt from the PPIPA. Hopefully this will be addressed as an outcome of the review.

To deal with these issues, the NSWFB Records Section is developing a policy that will require the researcher to give evidence of the permission of the person concerned or, if they are dead, their next of kin, to access their records. Access to sensitive information, such as medical or disciplinary records, will require explicit permission.

Community risk management programs

Under its Information and Communications Technology Strategic Plan, the NSWFB has, over the last two years been increasing the coverage of its computer network by installing a computer in every fire station for reporting, training and administrative purposes (this is separate from the connection of each station to the dispatch system).

Now that all staff have access to a computer, there is a growing demand for firefighters to collect information on community risk management activities, such as the installation of smoke alarms, fire safety programs in schools and presentations to community groups. To this end, the NSWFB is developing a Community Activity Reporting System (CARS) for reporting on prevention and preparedness activities, in the same way as we use the Australian Incident Reporting System to report on response and recovery activities.

CARS is not only used for performance reporting (number of activities, number of firefighters involved, etc) but will also be the repository for information about the subjects of the activities (eg name and address of smoke alarm recipient). Some of this information is personal, and some of it can get very sensitive, for example information collected on juvenile firesetters.

As Privacy Contact Officer, it is my role to advise the Community Risk Management Officers and others involved in the development of the community risk management programs and CARS on how to ensure that their collection and management of information complies with the PPIPA. For each program, for each field in CARS, it is necessary to go back to first principles and ask the *purpose* for which the information is being collected and used, and whether this is reasonable.

For example, it was proposed that when firefighters replace a battery under the Smoke Alarm Battery Replacement for the Elderly (SABRE) program, they collect information on the age of the recipient. Not surprisingly, firefighters were reporting difficulties with getting little old ladies to tell them their age, and were often leaving the field blank. Since eligibility for the program is normally determined by partnership organisations such as Meals on Wheels, there seems little value in collecting the information.

There was also a proposal to collect information on the mobility and other impairments of all the residents of the household. This is sensitive personal information, since it relates to health. It is also very difficult information to keep up-to-date and accurate, which is a requirement under Information Protection Principles 4 and 9. Firefighters were reporting that even basic information about residents of premises was normally inaccurate after one year, as elderly people are highly likely to move into other accommodation such as retirement villages or nursing homes. Their health status is likely to change even faster than their address. It was difficult therefore to see the value of collecting health information as well, and I advised against it.

In developing applications to collect information about members of the community, people should resist the temptation to collect information 'just in case it might be useful' for some hypothetical future program. The more personal information an organisation holds about an individual, the more resources the organisation must put into collecting it properly, keeping it up-to-date and accurate, storing it securely and making sure it is used appropriately. Holding personal information that you do not need puts you at a higher and unnecessary risk of a breach of security or privacy.

Application development

CARS is just one of a number of information applications currently being developed by the NSWFB. The NSWFB is committed to using information management and technology to make business processes more efficient to free up frontline firefighters from administrative tasks so that they can deliver better prevention, preparedness, response and recovery services. As many of the administrative applications being developed deal with employee information in some form, I have been involved with advising the project teams on privacy issues.

A good example is the development of Employee Self Service, where staff can check their personnel and pay details in the Human Resources Information Management System through the Employee Self Service site on our Intranet and update some fields, such as address and emergency contact information, online. Privacy management was an integral part of the security plan for this system, which includes encryption of data transmissions, logs of changes, password management, security and privacy notices on login screens and informative messages on view and edit screens.

The lessons learned from the development of Employee Self Service are now being applied to other applications such as a Workplace Hazard and Injury Notification System and a sick leave management system, and will be taken into consideration in the planned introduction of new human resources and knowledge management systems. Standards have been set for network and data security plans, use of test data, encryption, etc, which can be applied to all new developments. The positive reaction of staff to Employee Self Service is a measure of their trust in the security and privacy of the system. It is also enabling us to meet other Privacy Protection Principles by making our data more accurate, giving staff an easy way to access and correct their personal information, and giving them better information on what their details are used for.

Information security

Privacy management is one aspect of information security management. The NSWFB is currently moving down the path of certification to AS/NZS 7799.2:2003, *Information security management: specification for information security management systems* and has just completed an Information Security Management System Development Project. The work done in preparing the Privacy Management Plan proved an excellent foundation for considering information security. The audit of personal information assets made a good basis for a wider audit of all NSWFB information assets and gave a starting point for allocating security classifications to NSWFB information. Lessons learned from privacy management issues have been incorporated into the Information Security Plan. Awareness of privacy issues and privacy management practices made managers more receptive to discussion of information security issues. In the long term, privacy and information security management will be built into all NSWFB information systems and management practices.

What next?

The next major privacy project for the NSWFB is the introduction of the *Health Records and Information Privacy Act 2002* which came into force on 1 September 2004. This act removes health information about individuals from the jurisdiction of the PPIPA and makes it the subject of 15 Health Privacy Principles. The NSWFB now needs to review its personal information assets to identify which hold health information and assess whether there are any new actions that need to be taken to meet the requirements of the new act.

Conclusion

Privacy management is an ongoing issue in the NSWFB. Developments in information technology are making it easier to collect, store, manipulate and disseminate information. Privacy and security needs to be built into information systems at all stages of development. The community is becoming aware of how much data government and private organisations hold on individuals and is showing a growing concern about invasion of privacy and misuse of personal information. Employees also expect their privacy to be protected, and privacy breaches can severely disrupt the employer/employee relationship.

Privacy should not be seen as a barrier to doing business. Privacy is not an excuse for not carrying out reasonable human resource management practices or implementing community risk management programs. Ensuring that privacy management is built into processes and systems generally leads to a more effective outcome, since the data will be up-to-date and accurate and the people involved will be better informed about the purpose of the process and what the information will be used for. This builds trust between the organisation, its employees and the public.

References

1. Privacy NSW, http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipact, viewed 17 September 2004.

2. Pickles, A, 'Protecting exposures: privacy management in the NSW Fire Brigades', paper presented at the Australasian Fire Authorities Council Conference, Adelaide, September 2000.

3. Pickles, A, 'Trust me, I'm a firefighter! Why the new Privacy Act matters to the NSWFB', *Fire News,* February 2001, pp 33-35.

4. Pickles, A, 'Protecting exposures: privacy in an emergency', *Fire News,* Winter 2001, p 66.

5. Privacy Committee, *Code of practice for the use of* o*vert video surveillance in the workplace,* http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/code_overtsurveillance.pdf/$file/code_overtsurveillance.pdf, viewed 17 September 2004.

6. NSW Government, Exposure draft Workplace Surveillance Bill 2004, http://www.pco.nsw.gov.au/pdf/exposure/b04-027-20-d10.pdf, viewed 17 September 2004.

7. http://www.fire.nsw.gov.au/privacy.htm, viewed 17 September 2004.

8. Privacy NSW, *Submission by Privacy NSW on the review of the Privacy and Personal Information Protection Act 1998,* 2004, http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_ppipareview.pdf/$file/sub_ppipareview.pdf, viewed 17 September 2004, pp 64-66.

NSWFB policy on photographs and videos of dead or injured people

1. Introduction

At incidents, we do everything we can to minimise the impact of the incident on the people involved. The NSWFB has an excellent reputation for saving lives and providing help to the injured and distressed. It is important that this care for people is not jeopardised by invading their privacy unnecessarily or by displaying or publishing material that causes distress to the people involved, or their friends or relations.

Photographs or videos of dead or injured people are distressing to many people, including to firefighters. It is therefore the responsibility of everyone in the NSWFB to consider the implications carefully before taking, using or displaying this type of image.

NSWFB employees who take or use such images inappropriately may breach laws such as the *Privacy and Personal Information Protection Act 1998* or the *Occupational Health and Safety Act 2000*, or render themselves subject to internal disciplinary action.

2. When is it appropriate to take these images?

In most circumstances, there is no legitimate reason for NSWFB employees to take photographs of dead or injured people at incidents.

There are a limited number of circumstances where it is appropriate:

- Fire Investigators accredited by the Fire Investigation and Research Unit are permitted to take photographs or videos for the purpose of collecting evidence at a fire; and
- the Director State Operations may give permission for photographs or video footage to be taken at a major incident where there is an operational need.

At non-fire incidents it is not the NSWFB's responsibility to take photos or video footage for evidence.

3. Ownership of photographs and videos

All photographs and videos taken by NSWFB employees when on duty are the property of the NSWFB.

4. Public display of images

It is not acceptable to publicly display any images of dead or injured people. The only exceptions are when such images are presented in court or with the written permission of the Commissioner.

Public display includes:

- publication in NSWFB books, manuals, journals, videos, or other publications intended for use outside the NSWFB,
- publication in external publications such as newspapers, journals or conference papers,
- use of images on display stands at events,
- images displayed in NSWFB premises, including noticeboards, lockers, etc,
- images on Internet sites, and
- any other use where the images would be accessible by the public.

Note: An image does not have to contain a picture of a dead or injured person to be distressing. Consider the feelings of the people who may be viewing the image before using any image. In some cases, warnings may be appropriate.

5. Using images for training

The Manager Capability Training, in consultation with managers of specialist sections where appropriate, must approve any use of images of dead or injured people for training purposes.

The production of any training materials containing such images must be done through the Quality Education Support Unit.

6. Storage of images

Images of dead or injured people must not be kept at fire stations or on station computers. Station Commanders must check their stations for images of dead or injured people and ensure that any such photographs, videos or electronic files are destroyed.

If the Station Commander believes that an image may have some particular training value, they should contact the Manager Capability Training on (02) 9318 4303.

Any specialist section that is required to keep images of dead or injured people must ensure that:

- accurate records are kept of the images held,
- they are kept in a secure place,
- access to the images is restricted,
- film processing contractors are warned of the content of the film,
- users are warned of the content of the images before use, and
- images are securely destroyed when no longer required.