The Revised Study Design (2003-2006) – Privacy and Copyright

by David Patrao – for VITTA's Infonet publication – Issue 3 2002.

From the mid year PD, it is clear that there is some concern about what teachers need to cover in regards to Privacy and Copyright issues in both IPM and Systems, especially the need to cover a number of pieces of legislation.

The good news, is that you are not expected to turn your IPM or Systems class into a legal class – while the study design does make mention of particular legislation, it is important to note that students are only required to have a knowledge of the "key provisions" of the legislation – not an intricate knowledge.

From a teaching viewpoint, what we are trying to do is impart to the students the skills to become competent IT users and developers. They should have a sufficient understanding of the acts so that if they were in a position where they were dealing with data that is covered by these acts, they would be aware of their responsibilities under them. This is not to say that they would necessarily know the ins and outs of their responsibilities, but would be aware that they should seek out further information.

Much of what will need to be taught to the students is logical, especially if we start with the principle that people's personal data needs to be protected. Many of the provisions of the act merely legislate minimum safeguards that organisations need to apply to the collection, storage and dissemination of personal information. If we have started with the assumption that some data must be protected, it will fall into place quickly – as the logical response will suggest that we must do certain things to protect that data.

Information Processing and Management

Unit 3, Outcome 3 requires students to have a knowledge of the key provisions of the Privacy Act 1988 and the Privacy Amendment (Private Sector) Act 2000, the Information Privacy Act (Vic) (IPA), the Health Amendment Record Act 2001 (Vic) and the Copyright Amendment (Digital Agenda) Act 2000.

This outcome does not require the students to have a complete knowledge of the acts, but rather, that they have an understanding of how each act impacts upon an organisation that collects and uses personal data.

So what are the "key provisions"? In the absence of a document entitled "The key provisions of..." we need to make some judgement ourselves about what needs to be taught.

The Privacy Act 1988 and the Privacy Amendment (Private Sector) Act 2000

The Privacy Act has different guidelines for Government and non-Government Sectors. The Government Sector is the primary focus of The Privacy Act 1988, while the Privacy Amendment (Private Sector) Act 2000 deals with the private sector. While these are two separate acts, they

are closely linked, and in many ways are complementary. Students, while not needing to know all the specifics of each Act, need to be aware which act is applicable to different organisations.

The Government Sector
There are 11 Information Privacy Principles (IPP) that underpin this act in relation to the Government Sector. They are (with my interpretation of the content of the principle) :

Principle 1. Manner and purpose of collection of personal information
Personal information should not be collected for inclusion in a record or generally available for publication unless it is collected for a lawful purpose, function or activity directly related to collector and it is not collected by unlawful or unfair means.

Principle 2. Solicitation of personal information from individual concerned
The collector of personal information from an individual should make that individual aware ***before the collection (if practicable)*** of the purpose for which the information is being collected; if the collection is authorised by law (eg, the census); and any persons, body or agencies to whom the collector is likely to pass on this information.

Principle 3. Solicitation of personal information generally
The collector of personal information shall take all reasonable steps to ensure that the information that is collected is relevant to the purpose it was collected for, is up to date and complete, and should not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4. Storage and security of personal information
The record keeper should take all reasonable steps to ensure the data is protected from loss, unauthorised access, use, modification or disclosure or other misuse. And if the information is to be passed onto a third party, the record keeper must take all reasonable steps to ensure that the third party ensures the same.

Principle 5. Information relating to records kept by record-keeper
The record keeper shall take reasonable steps to ensure individuals can ascertain if their personal information is stored, and if so, the nature of the information, the main purpose the information is used for, and the action needed to access the information.

The record keeper should also maintain a record setting out the nature, purpose, classes of personal information kept, the duration it is to be kept and who has access to it. This record should be accessible by the public and needs to be forwarded to the Privacy Commissioner each year.

Principle 6. Access to records containing personal information
Individuals have the right to access information about them, unless this right is overridden by other laws.

Principle 7. Alteration of records containing personal information
The record keeper should ensure that processes are in place to ensure that information is kept accurate, up to date, complete and not misleading for the purposes it was collected. Where dispute over the accuracy of information occurs between an individual and the record keeper, and the record keeper elects not to change the information, then a memo to record a statement that the individual requested a change to be made be attached to the record.

Principle 8. Record-keeper to check the accuracy of personal information before use

Before the information is used, all reasonable steps should be taken to ensure that the information is accurate, complete and up to date.

Principle 9. Personal information to be used only for relevant purposes

The information that is collected should only be used for the purpose for which it was collected.

Principle 10. Limits on use of personal information

Information that was collected for a particular purpose cannot be used for any other purpose unless the individual has given consent to do so; there is reasonable grounds to believe the use in another purpose would prevent or lessen a serious and imminent threat to the life or health of the individual or other person; and the use is lawful.
Information may also be used for other purposes that are reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue. If information is used in this manner, the record keeper must ensure the record has a memo that notes this use.

Principle 11 Limits on disclosure of personal information

The personal information stored should not be disclosed to any person, body or agency (other than the individual concerned) unless: The individual is aware or reasonably likely to be aware that it would; the individual has consented; there are reasonable grounds to believe disclosure would prevent or lessen a threat to life or health; the disclosure is permitted under law or is necessary for the enforcement of criminal law; pecuniary penalty or the protection of public revenue.

Having read through that, I am sure you will have noticed a fair degree of repetition in the principles (and also the use of the word “information” when they really mean “data”, but that is a side point). I think from these principles, the key provisions of the Privacy Act, as it applies to Government Organisations, could be summarised as:

Data Collection: Information is collected in a manner that is lawful and those providing the information are informed as to the intended use of the information.

Data Processing, Storage and Maintenance: Agencies have an obligation to ensure that information is accurate, up to date and complete; there are processes by which individuals can access their own records and request alterations; information that is stored is secure and has access restricted to those who have legitimate purposes; and is only kept for a time frame that is reasonable in the context of the purpose the data was collected for.

Data Use: Data can only be used for the purpose it was collected – any other use must be accompanied by the consent of the individual it was collected from – unless there is threat to life or health, or in the enforcement of the law.

The Private Sector

The Private Act, in relation to the Private Sector, is based upon the National Privacy Principles (NPP). There are 10 NPP's. As with the IPP's that form the basis for the Government Sector, these cover the full range of activities that an organisation undertakes with people's data. Interestingly, where the guidelines to the 11 IPP that apply to the government sector is a 8 page document, the guidelines to the 10 NPP that apply to the private sector runs to 40 pages. The 10 NPP's (again with my summary following) are:

Principle 1: Collection

Organisations should only collect personal information that is necessary for one or more of its functions and activities. The information should be collected in a lawful manner, and if practicable from the individual concerned.

At the time of collection, or as soon as practicable after if this is not possible, the individual should be informed of: the identity of the organisation collecting the information and how to contact it; their access rights; the purpose of the information to be collected; whom the information might be disclosed to; any laws the require the information to be collected and the main consequences of not providing the information (if any).

If information is collected from a third party, reasonable steps must be taken to ensure the individual has been informed of the collection of the information and the details as listed in the previous paragraph, except if making the individual aware would pose a serious threat to the life or health of any individual.

Principle 2: Use and Disclosure

An organisation must not use or disclose information about an individual for any other purpose (a secondary purpose) other than the purpose for which the information was collected, except in a number of exceptions specified in the Act. Exceptions include (but is not limited to): where consent to do so has been obtained; the individual would reasonably expect the organisation to use the information for the secondary purpose; the secondary purpose is related to the primary purpose the information was collected; disclosure would prevent death or serious injury; the organisation suspects illegal activity and the information is disclosed to the appropriate authorities; or the disclosure is required under law.

It should be noted there are two notable exemptions to the disclosure principles above. They are where the secondary purpose is direct marketing, and when the disclosure is covered under the Health Amendment Act. The specifics of the Health Amendment Act will be looked at later. The Use and Disclosure principles in relation to direct marketing basically say it is acceptable to use information for direct marketing purposes providing the information is not sensitive. There are a series of rules direct marketers need to follow. Key aspect include: the individual has not made a request to the organisation not to receive direct marketing and when the information was collect the individual was given the opportunity to indicate this; in all direct marketing communication the individual must be given the opportunity to indicate they do not wish to receive any further direct marketing communication; and the contact details of the organisation must be contained in each direct marketing communication.

Where disclosure is made to authorities where illegal activity is suspected, or under the provisions of the Health Amendment Act, the organisation must keep a written record of the disclosure.

It is also important to note that when information on minors is collected, the rights afforded to the individual in this act are passed onto the parents or guardians, and this act does not over ride any existing obligations an organisation has not to disclose personal information.

Principle 3: Data Quality

An organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Principle 4: Data Security

An organisation must take reasonable steps to ensure that the personal information that it collects is protected from misuse such as unauthorised access, modification or disclosure, or loss. They must also ensure that that all reasonable steps are taken to destroy or de-identify personal information if it is no longer needed for the primary purpose it was collected for or it may no longer be used or disclosed under NPP 2.

Principle 5: Openness

An organisation must set out in a document a clearly expressed policy on its management of personal information and make this document available to anyone who asks for it. It must also, on request by a person, take all reasonable steps to let the person know what sort of personal information it holds, including the purpose, how it was collected, and how the organisation stores, uses and discloses the information.

Principle 6: Access and Correction

If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual. There is a very long list of exceptions – but they are generally common sense ones – such as where the request is frivolous or vexatious, the information relates to existing or anticipated legal proceedings, providing access would be unlawful etc. There are also provisions for the non-disclosure of commercially sensitive material, especially if that material was generated through analysis of the information by the organisation.

Where an organisation believes that it is not required to provide information when requested, it must provide an explanation for the refusal, and determine if there are suitable alternatives (such as the use of intermediaries) available that would meet the requirements of both parties.

Organisations must not charge individuals excessive fees for providing access to information, and may not charge an individual for lodging a request for access.

If any individual is able to establish that there are errors contained within information an organisation holds about him/her, the organisation must take all reasonable steps to correct the information. Where the organisation and the individual disagree on the accuracy of the information held, and the organisation declines to alter its records, the organisation must provide reasons for refusing to change the records and at the request of the individual must include a statement detailing the disagreement with the information.

Principle 7: Identifiers

Identifiers, such as a Tax File Number or Medicare number that are not generated by an organisation cannot be adopted by an organisation as a means of identifying an individual or

company. Note though, this does not mean it cannot be stored by the organisation, just that it cannot be used as a primary identification field.

The exception to this is the Australian Business Number (ABN).

Principle 8: Anonymity

Where it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

Principle 9: Transborder data flow

An organisation in Australia or an external Territory may not transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country without the consent of the individual except in specific circumstances detailed in the act (generally where is it impractical to obtain the consent) or where the recipient is in a country that has a law, binding scheme or contract which effectively upholds the NPP.

Principle 10: Sensitive Information

An organisation must not collect sensitive information about an individual unless the individual has consented, or the collection is required by law. There are a number of exceptions – relating particularly to Health research, and non-profit organisations, however, in all the exemptions, the expectation is that the information would not be disclosed without consent, nor kept for any period longer than required for the purpose it was collected.

As with the Government Sector, there is a large degree of repetition within the NPP. The key provisions, as applied to the Private Sector could be summarised as:

Data Collection: Data collection by organisations needs to be undertaken in a lawful manner, and individuals supplying the data need to be made aware of the purpose of the collection, and their rights in relation to the organisations use of the data. Data collection methods must also include a statement detailing the organisation's privacy policy and contact details, and the option to request that the data collected not be used for direct marketing purposes.

Data Processing, storage and maintenance: All reasonable steps need to be taken to ensure that the data that is collected is accurate, complete and correct. Data should be stored is a secure environment, with access restricted to those that have authorised purposes. Organisations have a responsibility to ensure that procedures are in place to allow individuals to view data stored about them, and to have corrections made if errors are detected. Organisations also need to ensure that these procedures are readily available.

Data Use and Dissemination: Data should only be used for the purpose it was collected for, although it may be used for secondary purposes if it reasonable to do so. It must be noted that the exception to this is direct marketing. It is acceptable to use data for direct marketing purposes, however, when this is done, individuals must be given the option of requesting not to receive any further direct marketing. Information should not be disseminated to other countries where similar privacy provisions do not exist.

As you can see, the basic principles that underpin both acts are essentially the same. The major difference is that government organisations operate under stricter controls regarding what can be done with the information collected – in essence, they can only use data for the purpose it was collected. Private organisations may use the information that is collected for secondary purposes

provided it meets the provisions contained within the act (and they are fairly wide provisions). Both the Government and Private organisations have obligations to ensure data is stored safely, is accurate and complete. They both must also have process whereby individuals can access (and correct if necessary) information contained about them.

The Information Privacy Act (Vic.)

The Information Privacy Act (Vic) is also based upon the NPP (although the act uses the term IPP). In essence the act provides the same protection as the Privacy Act 1988. The major area of difference here is the jurisdiction. The Privacy Act 1988 deals with Commonwealth Government Agencies and Private Organisations. The Information Privacy Act (Vic) deals with Victorian Government Departments, Agencies and their sub – contractors, as well as Victorian local government bodies and their sub- contractors. The provisions of the Victorian act are basically the same as the Commonwealth legislation. The important difference that students will need to be made aware of is who a particular organisation would be governed by. If the organisation in question is a Victorian Government Agency, local council or a sub contractor of them, then they will be covered by the Information Privacy Act (Vic). All other organisations are covered by the Commonwealth Act (other than the corresponding organisations in other states). The general rules are the same though, as they are based upon the NPP. One of the specific functions of the Information Privacy Act (Vic) is to establish the office of the Victorian Privacy Commissioner to oversee the compliance with the act.

The Health Records Act 2001 (Vic)

As with the Information Privacy Act, the Health Records Act 2001 (Vic) is based upon the NPP, so the same principles that underpin the Privacy Act 1988 are also applicable here. As with the Information Privacy Act (Vic), the major focus of the Act tends to be jurisdictional. This act covers both the government and private sectors, and details the rights of individuals and the responsibilities of organisations that hold information.

The most important aspect to note about this legislation, is that it allows a greater level of exemptions and exclusions than the other privacy legislation. This is because of the mandatory reporting of certain diseases. Conversely, it also provides for greater protection for the privacy of the individual's information if the disease is not covered by mandatory reporting. It also covers in greater detail the manner in which information can be used, especially in research.

The rights of an individual to view information held on them, and the processes to be followed are similar to those of the Privacy Act 1988.

Information Processing and Management and Information Systems

Unit 3 Outcome 3 of IPM and Unit 3 Outcome 3 of Information Systems require students to have an understanding of the key provisions of the Copyright Amendment (Digital Agenda) Act 2000. While obviously IPM and IS will take different views on the key aspects of the legislation, the legislation treats a computer program and other digital items (such as a web page) in a similar manner.

The Copyright Amendment (Digital Agenda) Act 2000

The Copyright Amendment (Digital Agenda) Act 2000 covers the various copyright issues that exist with digital media. This is a particularly lengthy document (as one would expect) that covers all aspects of digital copyright. There is no doubt that students are not expected to have a complete knowledge of the act – however, there are a few areas that it would be reasonable for us to expect students to understand.

Copyright Protection is Free and Automatic
There is no system of registration for copyright protection in Australia, and copyright protection is free and automatic. This also applies to non-Australian works published or accessed in Australia. A copyright notice (or the ©) while signifying copyright protection is not actually needed – items are protected even though the copyright notice is not on it.

Who Owns Copyright
The general rule is that the creator of the item is the first owner of copyright. This right can be varied by agreement, but there are also some specific exclusions that are relevant to digital items.

When the work is made by an employee in the course of employment, and as part of the employee's usual duties, then the first owner of copyright is the employer. This includes programs / websites / documents etc. that are written by an employee, but does not include those written in a freelance or contract arrangement.

The government is the first owner of copyright in material created or first published under its direction or control.
It is important to note that owning a disk or piece of hardware does not mean that you own the copyright to that material.

Rights of Copyright Owners
Owners of copyright materials, including computer programs and other digital forms, have a number of exclusive rights including the right to: reproduce the item in a material form (this includes copying the program to the hard disk of a computer, and writing or typing the source code of the program); publish the item (meaning to make the item available to the public for the first time in Australia); make an "adaptation" of the item (this includes making a version of the item in a different programming language, code or format); and communicate the program to the public (including by making it available online, or by electronically transmitting it including posting it on the internet.)

If anyone other than the copyright owner wants to do any of these things with the program / item, he or she will generally need the owner's permission. Copyright protection last for the life of the author plus 50 years. Note that the author is the individual or individuals that created the materials, not the company that published it. If there is more than one author, copyright will last for the life of the last surviving author plus 50 years.

Copyright Infringement
Copyright infringement in regards to electronic products occurs whenever protected material is dealt with in a manner that is exclusively controlled by the copyright owner. This can include making reproductions, making "adaptations" or something similar. Where a digital item has been made commercially available with a licensing agreement, actions that are in breech of that agreement would be an infringement of the copyright owner's rights.

Systems teachers should note:
Dealing with a "substantial part" of a computer program without permission in one of the ways controlled by the copyright owner may also infringe copyright. The term "substantial part" is not defined in the act, and it is left to the court to decide the question in regards to the specific circumstances of each case. The courts have adopted a qualitative as well as quantitative approach so that a small part may still be "substantial" if it is essential, important or vital in relation to the whole work from which it was taken.

Copyright is also infringed by someone who "authorises" someone else to infringe copyright.

In addition, a person may infringe copyright by importing computer programs (even legitimate copies) for sale or other commercial purposes without a licence from the copyright holder. It should be noted though, that some forms of digital media are no longer covered by this legislation, and "parallel importing' is now permitted (particularly in the case of music CD's).

Technological protection measures
It is illegal to make, import or commercially deal with devices and services which circumvent technological copyright measures (such as decryption software, or the chips in play stations). There are exceptions to this if it is for a permitted purpose.

Exceptions
There are a number of exceptions where permission from the copyright owner would not be required. These include:

Making a backup copy of a computer program – the legitimate owner of a computer program may make a backup copy of the program either to use in place of the original copy or to store in case of the original is lost or destroyed. This exemption does not apply if the licensing agreement of the software prohibits it or has expired, or the original program has a technological block to prevent the copying of the program. Further, this exemption only applies to computer programs – it does not apply to music CD's, computer games or CD-ROMS.

Making inter-operable products - a program may be adapted in order to get information necessary to enable an interoperable product to be made.

Security testing and error correction – a copy may be made for various security testing and to correct errors and security flaws.

Government use – the government may use copyright material without the copyright holders permission provided the use is "for the services of the government".

Other Issues
There are a number of other issues that are covered in this act, such as rights management, retransmission of free to air broadcasts and the liability of carriers and ISP's – however, they are not of significance to the study design.

When teaching about copyright issues, teachers should ensure that students are made aware of the rights of the copyright holder, and how as producers and consumers they could infringe them.

Students should be able to provide general responses to questions like:
If I wrote a computer program, who owns the copyright of it?

Is it an offence to copy program code?
Am I allowed to copy software?
Am I allowed to include pictures from a website in my website?

Acknowledgements:
The following were used in the writing of this article:
Internet: copying from
Digital Agenda amendments: an overview
Computer software and copyright
(All from the Australian Copyright Council)
Guidelines to the National Privacy Principles
Information Privacy Principles under the Privacy Act 1988
(From The Office of the Federal Privacy Commissioner)

Further Information:
www.privacy.vic.gov.au : Victorian Privacy Commissioner
http://healthrecords.health.vic.gov.au/overview.htm : Victorian Health Records Act
www.privacy.gov.au: The Office of the Federal Privacy Commissioner