**INB255/INN255 Security Workshop 3:**

1. The privacy act is concerned with the dealing of personal information and how it is used, and the manner in which it is collected.
2. An individual, a body corporate, a partnership , any other unincorporated association or a trust. It does not apply to a small business operator, an agency or a State or Territory authority.
   * 1. Personal information refers to: “means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.”
     2. Record refers to a:
        1. a document or
        2. a database (however kept); or
        3. a photograph or other pictorial representation of a person
     3. Sensitive information refers to:
        1. information or an opinion about an individual’s:
           1. racial or ethnic origin; or
           2. political opinions; or
           3. membership of a political association; or
           4. religious beliefs or affiliations; or
           5. philosophical beliefs; or
           6. membership of a professional or trade association; or
           7. membership of a trade union; or
           8. sexual preferences or practices; or
           9. criminal record;
        2. that is also personal information; or
        3. health information about an individual; or
        4. genetic information about an individual that is not otherwise health information.
   1. a generally available publication; or
   2. anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or
   3. Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act; or
   4. records (as defined in the *Archives Act 1983*) in the care (as defined in that Act) of the National Archives of Australia in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or
   5. documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980*; or
   6. letters or other articles in the course of transmission by post.
3. There are 11 principals.
4. A record keeper is required to do:
   1. that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
   2. that if it is necessary for the record to be given to a person in connection with the provision of a service to the record‑keeper, everything reasonably within the power of the record‑keeper is done to prevent unauthorised use or disclosure of information contained in the record.
5. Exceptions:
   1. the individual concerned has consented to use of the information for that other purpose;
   2. the record‑keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
   3. use of the information for that other purpose is required or authorised by or under law;
   4. use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
   5. the purpose for which the information is used is directly related to the purpose for which the information was obtained.
   6. There are 10 National Privacy Principles
      1. An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.
      2. On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.
      3. Yes they do
      4. Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.
6. D
   * 1. NPP 4.1
     2. A telecommunications company allowed individuals to access their mobile phone account information by calling a 1800 number, following the voice prompts and keying in the relevant mobile phone number. The account information available to the caller was the credit balance and transaction details of the last payment.
     3. In particular, the telecommunication company system would now only authenticate and process the incoming call when the calling number was the number of the account.
     4. 2.1
     5. The financial institution provided details of the deposit to the former partner, including dates and amounts. The former partner provided these details to the Child Support Agency for use in a reassessment of the complainant's income.
     6. The respondent agreed to issue a written apology to the complainant; conduct an analysis of the complainant's accounts across a specified timeframe to reassure the complainant that no other unauthorised disclosures had occurred; and counsel the staff member who had dealt with the former partner's enquiry. The respondent also paid compensation to the complainant after the parties signed a Deed of Release.
   1. The University monitors its information systems and services and carries out detailed security audits of systems, data and access as required. As a result, QUT logs network activity and may use it to investigate faults, security breaches and unlawful activity. Where diagnosis of problems, investigations or security audits are required, the University reserves the right to access individual files.
   2. Any breaches of security requirements by an individual user may result in disciplinary action (for staff and students) or the suspension or termination of access rights and computer accounts in accordance with the Acceptable use of information technology resources policy ([F/1.11](http://www.mopp.qut.edu.au/F/F_01_11.jsp)).
7. Sd
   1. HTTP cookies are files of text sent by a server to a web browser. They are then sent back unchanged by the browser every time it connects to that server. They are sometimes called web cookies or just cookies. HTTP cookies are used for security, making logs, and keeping some information about users. A cookie might be used to save your options on a website. The word "cookie" comes from the word "magic cookie". This is a well-known idea in Unix computing which inspired both the idea and the name of HTTP cookies.
   2. Persistent cookies are stored in a text file on the clients computer. Non-Persistent cookies are stored in RAM on the client and are destroyed when the browser is closed.
   3. D
      1. Both types. Weeks
      2. I found no cookies for QUT, but I don’t elect to keep them.
      3. Yes – some for forums, reddit, banking.
      4. No
   4. No need to relogin. Can keep preferences
   5. QUT obtains the following:
      1. the IP address of the computer you are using or an IP that is dynamically allocated by your internet service provider
      2. the date and time of your visit
      3. the pages accessed and documents downloaded
      4. the file size of the pages downloaded
      5. the type of browser used and screen resolution
      6. the referring page (ie last page visited before entering the QUT site).
   6. Single pixel gif technology
   7. No
8. 1. Can commit crimes using another persons identity thus preventing him releasing his own.
   2. Social engineering (i.e. just tricking the victim into releasing information), keylogging (monitoring there computer using either hardware or software solutions for keystrokes in the hopes of getting access to passwords/login details)