SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Outline solutions for Week 4 Tutorial Qs for L3: Privacy and Security

QUESTION 1

The Australian Privacy Act 1988 is available from the Office of the Australian Information Commissioner (see http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act). Use the information from the Australian Information Commissioner's page, or access the Privacy Act 1988, to answer the following questions:

a) What sort of privacy is this Act concerned with?
b) Which organizations does the Act apply to?
c) Referring to Section 6 in this Act (in Part II Interpretation), what do the following terms or phrases mean?
    i. personal information
    ii. record
    iii. sensitive information
d) What is not regarded as a record under this Act?
e) How many *Information Privacy Principles* (IPPs) are there (see Section 14 - in Part III Information Privacy)?

Privacy Act 1988:

a) Concerned with information privacy or data privacy.

b) Australian federal government agencies and ACT government agencies.

c) Section 6 terms or phrases:

i. <u>Personal information</u> 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.

ii. <u>Record</u> means a document; or a database (however kept); or a photograph or other pictorial representation of a person

iii. <u>Sensitive information</u> means

i. information or an opinion about an individual's:
(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of professional or trade association;
(vii) membership of a trade union; or
(viii) sexual preferences or practices; or
(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

d) <u>Not regarded as a record</u>: Look under 'record' in Section 6 for exclusions:
(d) a generally available publication; or
(e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or
(f) 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
(fa) 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
(g) 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
(h) letters or other articles in the course of transmission by post.

e) There are 11 *Information Privacy Principles*.

QUESTION 2
In 2000 the Australian Privacy Act 1988 was amended to include National Privacy Principles. Use the information from the Australian Information Commissioner's page, or access the Privacy Amendment (Private Sector) Act 2000, to answer the following questions:

a) What was the purpose of the 2000 Amendment?
b) How many *National Privacy Principle*s (NPPs) are there?

Privacy Amendment (Private Sector) Act 2000:

a) Extended coverage of the Privacy Act 1988 to the private sector (some exemptions)
b) Has 10 National Privacy Principles

QUESTION 3
In 2012 there was another Amendment; the Privacy Amendment (Enhancing Privacy Protection) Act 2012. This amendment provides 13 *Australian Privacy Principles* (APPs) to replace the previous IPPs and NPPs. Use the information from the Australian Information Commissioner's page, or access the Privacy Amendment (Enhancing Privacy Protection) Act 2012, to answer the following questions:

a) Under APP1, entities must have a clearly expressed policy about the management of information. What must the privacy policy contain?
    i. Use your web browser to go to the home pages of some well known organizations: QUT, your bank, Google, or well known Australian retailers. **Look at their privacy policies**. Do they comply with the Privacy Act?

b) APP5 is concerned with notification of the collection of information. What must entities collecting personal information do in order to comply with this principle?
c) APP 6 imposes limits on the use or disclosure of personal information. Under this principle, an entity who holds personal information that was obtained for a particular purpose shall not use the information for any other purpose, although there are exceptions. List the exceptions.
d) APP11 covers the security of personal information. If an entity holds personal information, what does this principle require them to do?

Privacy Amendment (Enhancing Privacy Protection) Act 2012:

a) APP1 requires an APP entity to have a clearly expressed and up-to-date policy about the management of personal information by the entity, which must contain the following information:
   a. the kinds of personal information that the entity collects and holds;
   b. how the entity collects and holds personal information;
   c. the purposes for which the entity collects, holds, uses and discloses personal information;
   d. how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
   e. how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
   f. whether the entity is likely to disclose personal information to overseas recipients;
   g. if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

b) APP5 states that at or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take reasonable steps:
   i. to notify the individual of details regarding the collection; or
   ii. to otherwise ensure that the individual is aware of any such matters.

   Matters for notification include:
   a. the identity and contact details of the APP entity;
   b. if:
      i. the APP entity collects the personal information from someone other than the individual; or
      ii. the individual may not be aware that the APP entity has collected the personal information;

   the fact that the entity so collects, or has collected, the information and the circumstances of that collection;
   c. if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order
   d. the purposes for which the APP entity collects the personal information;

e. **the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;**
f. **any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;**
g. **that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;**
h. **that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;**
i. **whether the APP entity is likely to disclose the personal information to overseas recipients;**
j. **if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.**

c) **APP6: Information collected for a particular purpose should not be used for any other purpose, although there are exceptions:**

a. the individual concerned consented to use or disclosure of the information; or

b. the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

i. **if the information is sensitive information—directly related to the primary purpose; or**
ii. **if the information is not sensitive information—related to the primary purpose; or**

c. **the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or**
d. **a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or**
e. **the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or**
f. **the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.**

d) **APP11:**

If an APP entity holds personal information, they must take reasonable steps to protect the information:

a. **from misuse, interference and loss; and**
b. **from unauthorised access, modification or disclosure.**

If:

c. **an APP entity holds personal information about an individual; and**
d. **the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and**
e. **the information is not contained in a Commonwealth record; and**
f. **the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;**

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

QUESTION 4

Complaints about breaches of the Privacy Act can be made to the Information Commissioner, and may be investigated. Case notes of (de-identifed) finalized complaints considered to be of interest to the general public are published by the Office of the Australian Information Commissioner. From the Homepage of the Office of the Australian Information Commissioner (http://www.oaic.gov.au), select *Privacy*, then *Applying privacy law, Privacy case notes,* and then select *List of privacy case notes*. From the published case notes for 2011:

a) Examine the Case Notes for the case **H and Registered Club [2011] AICmrCN 2** and answer the following questions:
   i. Which Privacy Principles are alleged to have been breached?
   ii. How did this alleged breach occur?
   iii. What was the outcome of the investigation?
b) Examine the Case Notes for the case **P and Retail Company [2011] AICmrCN 10** and answer the following questions:
   i. Which Privacy Principles are alleged to have been breached?
   ii. How did this alleged breach occur?
   iii. What was the outcome of the investigation?

Case notes: breaches of the Privacy Act:

a) H and Registered Club [2011] AICmrCN 2

i. National Privacy Principles 1.1, 1.3 and 4.2:

- **NPP 1.1: an organisation must not collect an individual's personal information, unless that information is necessary for one of more if its functions or activities.**
- **NPP 1.3: at … the time an organisation collects an individual's personal information, it must take reasonable steps to ensure an individual is aware of … the purposes for which the information is collected.**
- **NPP 4.1: an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.**

ii. The club scanned the driver's licence of patrons. The information that the club was (legally) required to collect was name, address and signature. However, by scanning licences, the club was collecting

additional information date of birth, driver's licence number, driver's licence type and photograph. The complainant was also concerned that the club did not adequately inform patrons regarding the purpose of collection, or the security of storage.

iii. The outcome of the investigation was conciliation: the club:

- **Offered to delete the complainants' information from their database and accept a statutory declaration of name, address and date of entry,**
- **agreed to offer an alternate manual register signing process, and**
- **agreed to delete the information for other patrons (replace with statutory declarations) if they chose to.**

The Commissioner considered the respondent dealt with the matter adequately and closed the case.

b) P and Retail Company [2011] AICmrCN 10

i. NPP1.1 and 1.2:

- **NPP 1.1: an organisation must not collect an individual's personal information, unless that information is necessary for one of more if its functions or activities.**
- **NPP 1.2: must only collect information by lawful and fair means**

ii. P claimed that a retail company recorded outbound calls made to them without notifying them that it was recording the calls.

iii. The Commissioner investigated and found that the recording of the calls by the retail company was necessary for one of the company's functions, so it was not in breach of NPP1.1. However, the Commissioner found that there was a breach of NPP1.2 as the company did not provide sufficient notification that collection of information via call recording would occur, so collection was unfair and unlawful. The retail company changed its procedures and offered to apologize to P.

QUESTION 5

The Australian Information Commissioner may instigate investigations into potential privacy breaches. These own motion investigation reports are published by the Office of the Australian Information Commissioner. From the Homepage of the Office of the Australian Information Commissioner (http://www.oaic.gov.au), select *Privacy*, then *Applying privacy law,* and then select *Commissioner initiated investigation reports*.

a) Examine the report for **Telstra Corporation Limited in June 2012** and answer the following questions:
   i. Which Privacy Principles are alleged to have been breached?
   ii. How did this alleged breach occur?
   iii. What was the outcome of the investigation?

b) Examine the report for **AAPT and Melbourne IT in October 2013** and answer the following questions:
   i. Which Privacy Principles are alleged to have been breached?
   ii. How did this alleged breach occur?

iii. What was the outcome of the investigation?

Case notes: breaches of the Privacy Act:

a) Telstra Corporation Limited [June 2012]

i. National Privacy Principles 2 and 4:

- **NPP 2: an organisation must only use or disclose personal information for the primary purpose for which it was collected, unless exemptions apply.**
- **NPP 4.1: an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.**

ii. A Telstra tool which accessed customer information from an internal database was accessible online. Personal information of Telstra customers, including names, phone numbers, order numbers and some other information (passwords, date of birth, passport numbers, credit card number) was publicly accessible.

iii. The Commissioner determined that:

- **disclosure of customer personal information occurred on a large scale over a long period of time, in breach of NPP2.1. This was a result of a series of errors in Telstra's reporting and monitoring systems.**
- **Although Telstra had existing policies and practices in place that would have prevented the errors that lead to the disclosure, the organization did not appear to be acting on them. Unathorized access could occur. Telstra therefore did not have reasonable steps in place with respect to data security.**
- **Telstra did act to secure customer data and committed to specific actions regarding reviewing and improving internal procedures.**

b) AAPT and Melbourne IT [October 2013]

i. National Privacy Principles 1.1 and 1.2:

- **NPP 2.1: an organisation may only use or disclose information for the primary purpose of collection, unless exception applies.**
- **NPP 4.1: must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.**
- **NPP 4.2: Personal information no longer required should be destroyed or de-identified. P claimed that a retail company recorded outbound calls made to them without notifying them that it was recording the calls.**

ii. A server holding AAPT information (but managed by Melbourne IT) was compromised by hacker group Anonymous and unauthorized data transfers occurred. Customer data was published on the Internet.

iii. The Commissioner investigated and found that:

- **There was not a breach of NPP2.1 as the customer data was made public through the malicious actions of Anonymous.**

- **There was a breach of NPP4.1, as AAPT did not appropriately manage and protect the information and did not have contractual measures in place to ensure customer data was protected. Additionally, they were using old versions of software with known vulnerabilities.**
- **There was a breach of NPP4.2, as not all of the compromised data was in use. AAPTs data retention policies were not being followed.**

QUESTION 6

Many organizations monitor the use of information assets by employees and other entities. At QUT, information assets are monitored, and security audits are also conducted periodically. Refer to Section F/1.2.7 of QUT's Manual of Policies and Procedures (http://www.mopp.qut.edu.au/F/F_01_02.jsp#F_01_02.07.mdoc) to answer the following questions:

a) What sort of monitoring does QUT perform?
b) What are the logs of this activity used for?
c) What are the potential consequences for misuse of QUT information assets?

QUT monitoring of information assets:

a) QUT monitors information systems and audits systems, data and access. QUT logs network activity, and where required to diagnose problems, may access individual files.
b) The logs of network activity may be used to investigate faults, security breaches and unlawful activity.
c) Potential consequences for misuse include disciplinary action, suspension or termination of access rights, or legal action (if actions constitute a crime under appropriate legislation).

QUESTION 7

Many internet applications use cookies for session management. Answer the following questions about cookies:

a) Explain the information transfer that takes place when cookies are used (the sort of information that is transferred, the source and the destination).
b) What is the difference between persistent and non-persistent cookies?
c) Locate cookies on your machine (The storage location varies depending on your browser, so search for the folder or file named Cookies or cookies).
    i. What type of cookies did you find (persistent or nonpersistent)?
    ii. For persistant cookies, how long have some of them cookies been on your machine? What are they associated with?
    iii. Did you find any cookies for QUT? Read the information on the use of cookies at QUT (http://www.qut.edu.au/general/privacy.jsp#1). What sort of information is stored in these cookies? Would this be regarded as personal information, as defined in the Privacy Act?
    iv. Did you find cookies for any other organizations that you regularly visit? Which?

v. Did you find any cookies for organizations you don't recognize?

d) The use of cookies can be beneficial for the user. Explain some of the beneficial uses.
e) Cookies can also be used in ways that may be regarded as invasive, and potentially a threat to user privacy. Explain how cookies set by third parties can potentially be used to profile the online interests of a user.

Cookies:

a) When cookies are used, information is transferred from the web server to the user's machine. This is a small text file that could include login name, subscription identifier, etc. This information can then be retrieved by the web site, so that the web server can keep state for the user.
b) Cookies can be persistant or not persistant.
  i. Persistant cookies are valid for multiple sessions. These contain an expiration date, and remain on the user's machine until the expiration date, or until they are deleted by the user.
  ii. Cookies without an expiration date are only valid for that browser session and are erased when the browser session is closed.
c) Look for persistant cookies for some shopping and information sites: typical format of the cookie file names is username@websitename, for example simpson@amazon.txt. You might see persistent cookies for third party advertisers also, such as doubleclick or adrevolver.
  i. Cookies at QUT: store visitor number and IP address, and if you authenticate to QUT, store a unique identifier, full name, email alias, relationship to QUT (staff, student, course, etc).
d) Beneficial use: the cookies help the web server track the user as they visit multiple pages, or possibly on multiple visits to the web site (so it can remember you). This can be used so that you don't have to authenticate every time you access a new page, for example.
e) Potentially invasive use: where web server sets a cookie that transfers information to a third party (often marketing analyst or advertiser) who can use that to profile your web browsing across sites that may seem to the user to be unrelated.

QUESTION 8

Web bugs are often used to track user visits to web sites.

a) QUT uses such tracking mechanisms, and provides information on the details collected in this manner under the heading 'Site usage' in the privacy and security statement available at http://www.qut.edu.au/general/privacy.jsp#1. What details does QUT obtain in this manner?
b) What sort of technology does QUT employ for the web bug?
c) Visit the QUT homepage, and find out where the content on the displayed page is coming from (For MS-IE users, choose View -> Webpage Privacy Policy). Is there any content on the QUT homepage that is not from QUT?

d) Visit the homepages of at least five well-known organizations: (your bank, news and weather services, well known retailers such as Myer and David Jones, other sites you commonly visit).
   i. Do any of these organizations have content provided by third party providers? Who is the third party?
   ii. Do any of these sites have third party providers in common?
   iii. Did you find any organizations that don't use third party content providers?

Web bugs:

a) **Details obtained by QUT's use of 'single pixel gif technology' include:**

   i. IP address of your computer (or an IP dynamically assigned by your ISP);

   ii. date and time of visit;

   iii. pages accessed and documents downloaded;

   iv. file size of downloaded pages;

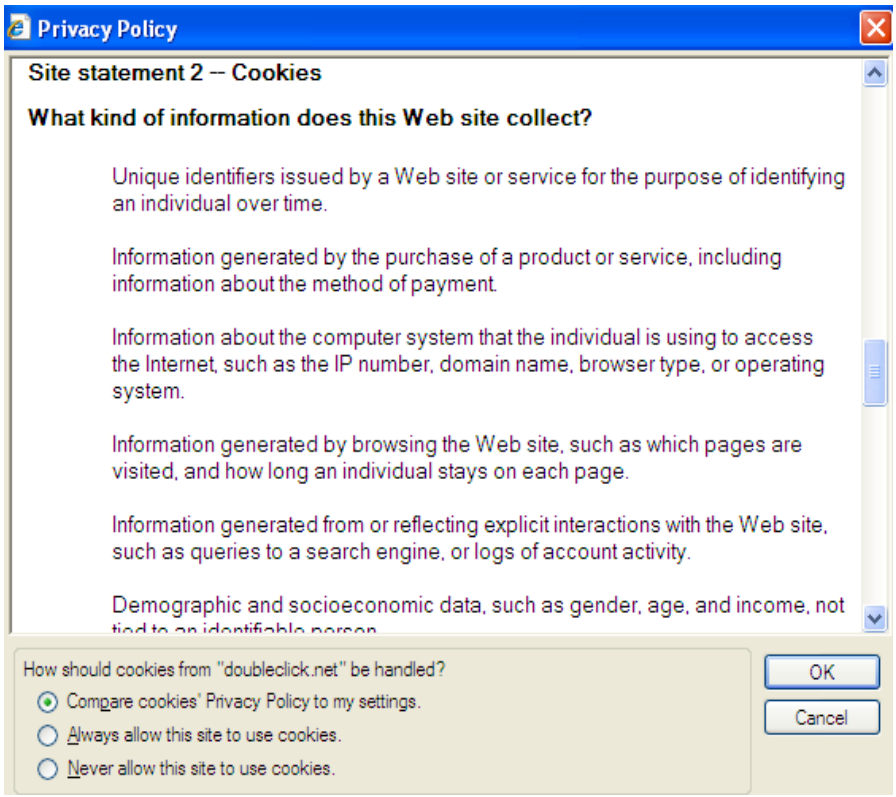
   v. browser type and screen resolution;

   vi. the referring page (ie the page you visited directly before you entered QUT's site)

b) QUT uses 'single pixel gif' technology.
   i. When a web page or email containing a web bug is requested, the web browser or email client sends a request to the servers for the content required to display the page or email. This includes the server that provides the web bug, which may be only 1 pixel in the page or email. The requests typically include other info, as outlined for QUT above and maybe the existence of any cookies previously set by that server on the client machine. The server can store all of this information in a database, associated with a unique identifier.

c) QUT homepage: Couple of references to content from 'googleadservices…'

d) THE BANKS:
- **ANZ bank has content from Google's Doubleclick (http://googleads.g.doubleclick.net/ …) Follow this trail and look at the privacy policy for (Google) Site statement 2 Cookies.**

- 

- **Content on the homepage for Commonwealth Bank of Australia (http://www.commbank.com.au/) includes content from 'Doubleclick' (owned by Google), another digital marketing firm 'Omniture' (owned by Adobe) - although the Omniture content is harder to spot. Follow the trail from https://cba.d2.sc.omtrdc.net/b/...) and also content from 'Adconion Media Group'.**
- **National Australia Bank (http://www.nab.com.au/) has content from 'Omniture' (although to find the Omniture content you have to follow the trail from http://smetrics.nab.com.au/b/ss/ ... to see that it is Omniture). NAB also has content from LivePerson. Check their privacy statement to see what they may use your information for.**
- **Westpac pages include content from Omniture (follow https://smetrics. ...) and from Facilitate Digital (http://adsfac.net/ …).**
- **Citibank (https://online.citibank.com/US/Welcome.c) has content from Google's Doubleclick, as well as Omniture (follow the https://metrics1.citibank.com.au/b/ss/... link) and Amazon services.**

NEWS and WEATHER

- **ABC news (http://www.abc.net.au/news/) has content from Google (DoubleClick) and RedSheriff (follow the http://secure-au.imrworldwide/... link) (An online ad company bought by Nielsen ratings company)**
- **The Australian Bureau of Meteorology homepage http://www.bom.gov.au/ includes content from 'Rubicon' and 'DoubleClick'.**

RETAILERS

- **Content on the Woolworths page (http://www.woolworths.com.au/) includes content from 'Googleadservices' and 'DoubleClick'.**
- **Content on the Myer webpage includes content from 'Coremetrics' (digital marketing analysts - now owned by IBM),**
- **Content on David Jones page includes content from 'Googleadservices', 'DoubleClick' and 'Coremetrics'**
- **Apple (http://www.apple.com/au/) has content from Omniture (follow the http://metrics.apple.com/b/ss... link)**
- **Google search page has the least amount of content: just from Google!**

QUESTION 9

Identity theft is a criminal act that involves one person using the personal identifying information of another in an attempt to impersonate them.

a) Explain the advantages an attacker gains by doing this.
b) Describe the methods an attacker can use to gain another person's personal information.
c) From the *Identity Theft* section of the Australian Competition and Consumer Commission (ACCC) SCAMwatch website (available at http://www.scamwatch.gov.au/content/index.phtml/tag/identitytheft) identify online scams which target personal information.

Identity theft: fraudulently obtaining proof of another's identity and impersonating them

a) Advantage is that attacker can obtain goods and services on credit but person being impersonated will acquire the debt, or attacker can perform illegal acts and person being impersonated may receive the punishment (e.g. speeding fines, etc)

b) Can gain information by
   a. 'Dumpster diving' for credit card receipts, pre-approved credit forms, etc
   b. Social engineering using phone calls, email messages etc
   c. Obtaining credit reports on victims
   d. Using Internet to get personal information from various sources: websites, publications
   e. Attacking databases holding personal information

c) These include phishing scams, phoney fraud alerts and bogus job opportunities.