**INFO 30006 GROUP ASSIGNMENT 2019**

**Vanessa Teague, Suelette Dreyfus & Heidi Tscherning**

**\*\*\* DUE DATE:** **Mon 7th Oct at 10am \*\*\***

The aim of this assignment is for you to examine the technical facts or political controversy over something with significant security and privacy implications. You will think about how the public debate was informed (or not) by accurate technical facts, and consider what technical or policy changes would improve the system.

This group project is worth 40% of your marks in INFO30006. You should work in groups of 3 or 4 - by now, all groups should be organised. Please let us know if you’re not part of a group of the right size all contained within the same workshop.

The task consists of two parts:

* 1. (10%) A 10-12 minute talk delivered in weeks 6 & 7. This is meant to be a work in progress, summarising your preliminary findings and explaining what further investigations you intend to undertake.
  2. (30%) A written report of *at most 6 pages*, in at least 12 point font, as a .pdf.

Questions and discussion should be via the LMS - there will be a dedicated discussion board.

Your group should choose one of the questions below. Some require a policy or politics essay, others are more technical. Ideally, it would be nice if groups in the same tutorial pick different questions, but this is not compulsory.

You will be judged on the depth of your research and the quality of your examination of different sides or options. In each case, you are expected to justify your answers with reasons, references, etc, even if the question does not explicitly say “explain your reasons” or “justify your answer.”

**Q1. The politics of security and privacy:** I**nquiry into press freedom**

Read some of the submissions to the Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press at: https://www.aph.gov.au/Parliamentary\_Business/Committees/Joint/Intelligence\_and\_Security/FreedomofthePress

We particularly suggest starting with

* 8, from the Australian Human Rights Commission,
* 21, from the Australian Federal Police,
* 32, from the Departments of the Attorney General and Home Affairs, and
* 38, from the ABC.

but you should also read any others that seem interesting.

1. Summarise the discussion in general terms, noting which submissions you’ve read.
2. Do the submissions fall roughly into two (or more) sides? For each side, explain the main points they make and identify one important argument you agree with, and one important weakness or limitation.
3. Find at least one important disagreement on a matter of *fact.* Identify
   1. at least one clear (or as clear as you can find) statement on each side of the dispute, with references/web links,
   2. the core issue at the centre of the dispute,
   3. the factual resolution, if there was one.

Write a short summary in your own words of who said what, and why, and what the truth was, as far as you can tell.

d. Consider one specific change to legislation, either one that was recently made (e.g. in the AA Act), or one that is proposed in one of the submissions you’ve read, or one you’ve thought up yourself. Discuss

1. why the change was (or should be) made,
2. a possible benefit,
3. a possible problem or risk,
4. some alternative approaches for achieving the same objective, with some comparison of options.

**2. The economics of consumer privacy: the Consumer Data Right.**  Look at the recently-passed bill introducing the Consumer Data Right <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6370>

You don’t have to read the whole thing, and you might find the Explanatory Memorandum more useful than the legislation itself.

1. Summarise the main ideas and objectives of the Consumer Data right. Do you think it will meet its objectives? Explain why or why not. Do you think it will have other consequences too? Explain what and why.
2. Identify at least one of each of:
   1. a significant benefit for individual consumers
   2. a significant benefit for the wider society
   3. a significant risk for individual consumers
   4. a significant risk for the wider society
   5. a significant risk or benefit for someone other than the three parties directly involved in the transfer of a consumer’s data (i.e. the consumer, the bank, and the party receiving the data).
3. Find at least one important dispute or disagreement about some (practical or political) aspect of the CDR. Identify
   1. at least one clear (or as clear as you can find) statement on each side of the dispute, with references/web links,
   2. the core issue at the centre of the dispute,
   3. the factual resolution, if there was one.
4. Identify at least one aspect of the CDR that remains poorly defined, unspecified or incompletely determined. Explain
   1. what the issue/term/idea is
   2. what the possible definitions or interpretations are
   3. how you think it should be defined or implemented.

**3. The technical details of Cloud storage.** Suppose you’re in charge of the government data cloud.

1. Explain the main requirements, examining confidentiality, integrity, availability and anything else you can think of.
2. Discuss what technical means you would use to achieve them and what tradeoffs you might have to consider. Consider the distinction between encryption in which the only data owner knows the decryption key, and encryption in which the storage provider knows the decryption key.
3. Who are the main attackers? Write at least three examples of a possible attack scenario, including its motive and likely perpetrator. Describe how your defence mechanisms would (or wouldn’t) defeat the attack.
4. Read the Digital Transformation Authority’s Secure Cloud Strategy at<https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/cloud/secure-cloud-strategy.pdf>

For each of the first two myths, that “The Cloud is not as secure as on premise services” and that “Privacy reasons mean government data cannot reside offshore,”

i. Give at least one argument in favour of the truth of the proposition, and one argument against.

ii. Summarise the argument given in the Strategy. Do you accept the argument or not?

iii. The “Myth” that “Privacy reasons mean government data cannot reside offshore” is ambiguous about whether it means that privacy law prohibits offshore storage, or whether good privacy practice implies that offshore storage is risky or stupid. Redo questions i and ii with whichever interpretation you didn’t use the first time.

4. **Technical comparison of metadata-hiding SMS.**

Note: this is a hard question in which you’ll need to think carefully about the cryptography involved in different systems. The idea is to compare three metadata-hiding Instant Messaging systems: Briar, Cwtch and Richochet refresh. Read the information on

* Briar <https://briarproject.org/how-it-works.html>
* Cwtch: <https://cwtch.im/>, particularly the whitepaper at <https://cwtch.im/cwtch.pdf>
* Ricochet refresh: <https://ricochetrefresh.net/> including the technical design notes at <https://github.com/ricochet-im/ricochet/blob/master/doc/design.md>

As you can see, the quality of the documentation varies a lot.

1. For each project, see if you can find a clear statement of
   1. what privacy properties are guaranteed, and
   2. what attackers are defended against.

For example, if you were looking at Signal you would say, “Signal preserves the privacy of the content of the messages, except against an attacker that actively interferes with the initial message exchange before the participants have checked their safety number.” Try to be as detailed as you can, and note that there might be different kinds of protection against different attackers. Of course, Briar, Cwtch and Ricochet all try to preserve both content and metadata.

b. Compare the different security/privacy properties. Are some better than the other(s)? Can you see any advantages or disadvantages among the three?

c. For each project, write a short (half-page) summary of the main idea of how *metadata* is protected. (Never mind about content.)

d. If you were a law enforcement or intelligence officer attempting to learn who communicated with whom over these systems, what would you try? List at least 3 ideas, and explain why they might (or might not) work. It’s fine if some of your ideas only work for one system and not the others.

**5. Field study of consumers’ privacy in shopping malls.**

For this option, you will need to do some online research of the digital advertisers’ offerings, as well as a site visit to at least one site.

1. Describe what surveillance occurs technologically of consumers in shopping malls such as Emporium, Westfield Doncaster, Chadstone (or other malls). Think facial surveillance, wifi tracking, smart kiosks etc.
2. Explain what surveillance is possible with existing infrastructure, and what surveillance is occurring, as far as you can tell. For example, are there links to credit card/debit card usage?
3. On site, test whether you get different offerings than others in your group.
   1. Is there is any obvious cause of the different offerings/prices/steerage to certain products?
   2. Are the ads targeted?
   3. Do you see the same ads?
   4. Do you see the same prices?
4. What consent do the customers give or not give?
5. What do the privacy policies or public notices say or not say?
6. Can you identify any examples in which you believe that the data is being collected or used in a fashion that is not consistent with the consent given?

**Submission instructions**

Submit on the LMS by Mon 7th Oct at 10am. Detailed submission instructions will be provided before the due date.

**Extensions / Late Submissions**

As this is group assignment, applications for extensions will only be considered in very exceptional circumstances.  If you are unwell or unavailable for a period of time it is your responsibility to communicate with your group.  Illness or other issues affecting a single group member will not be considered grounds for an extension.  Any applications for an extension should be made to the subject coordinator at least 72 hours before the submission deadline.

Late submissions will not be accepted unless an extension application has been approved before the submission deadline. Every member of the group is responsible for ensuring the assignment has been submitted on time.

**Academic misconduct, plagiarism, etc**

The University misconduct policy applies. All submitted work must represent the group’s understanding of the topic. The subject staff take plagiarism very seriously. In the past, we have prosecuted several students that have breached the university policy. Often this results in receiving 0 marks for the assessment, and in some cases, has resulted in failure of the subject.

You may use any sources you can find, as long as you properly attribute them.

You may discuss the project within your group.

You may ask and answer questions on the LMS, about any topic you like.

You may *not* discuss the project with anyone outside your group, even other students in the subject, except during your workshop presentation. (This policy aims to encourage discussion, but make it fair - do the discussion on the LMS, so everyone can learn from it.)