UNIVERSITY OF TECHNOLOGY SYDNEY

31272 Project Management and the Professional

Assignment 1 – Autumn 2016

Marks:	**20 marks (20%)**
Submission Components:	**Hardcopy Report**
Submission Due:	**5pm Monday, 2 May 2016**
Report Submission To:	**Assignment box CB11 (hardcopy) / UTSonline (softcopy)**
Length:	**2,200 -2,500words (of report body)**
Anticipated Commitment:	**12 hours per student**
Objectives/Graduate Attributes:	**4, 5 / A1, B3, B4, B6, E1, F1, F3**

This is an individual assignment

Technology development is occurring swiftly. In particular, the significant increase in Internet traffic has prompted the Australian government to pass legislation forcing Telcos to collect 'metadata' for use by official agencies – thus allowing those agencies to audit/monitor people's online activity. While value to national security and law enforcement might be apparent the ethics behind such a capability is still open to debate.

Background

In this assignment you will discuss the ethics of a real-life situation as reported in the public domain (see the attached case study). In this case, the recent passing into Australian law of a directive for telecommunications providers to collect and store user internet data for up to two years. As a project management student who in future may have privileged access to information such issues could be quite relevant to your long-term roles and activities within the technology sector.

While the original text for the case study news reports can be found in the references provided you are also expected to further research and investigate this topic for yourself.

Tasks and Assessment

This assessment requires that you prepare a report addressing the following questions in each section. You are expected to conceptualise the problem or issue, find relevant references for context, facts, theory and examples and come up with appropriate points of view. Your positions should be supported with argument and citations as appropriate. Marks will also be awarded for presentation and professionalism of response.

1) Stakeholder Ethics (8 marks)

a) Identify at least 3 key stakeholders relevant to this case study. For each key stakeholder describe the situation and reasoning from their perspective.

b) Explain the major areas of conflict, if any, between these perspectives.

c) For each stakeholder group identified, select what you believe is the relevant ethical view taken (i.e. choose from the 7 'ethical principles' given on slide 10 of lecture 2) – and then explain why you attributed that ethical stance to them.

d) What do you personally think of the circumstances described in the case study? Explain your own individual ethical view regarding the situation outlined and give your personal assessment of stakeholder groups involved. Are they justified in their points of view?

2) International Codes of Ethics (6 marks)

Many could potentially be affected by government agencies being able to track their internet activity. Research the ethics and codes of conduct for **Information Technology** industry bodies representing **Australia** (e.g. Australian Computer Society (ACS)) plus **one other nation** or international groups (e.g. Association for Computer Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), British Computer Society (BCS), Computer Society of India (CSI), Institute of IT Professionals, New Zealand (IITP), etc.).

Answer the following questions:

a) What evaluation would each Code likely render on the case study situation described? Which (if any) stakeholder position would the Codes most likely support? Supply clear reasoning for both these points.

b) What are the major differences (if any) between the ethical codes of conduct you have reviewed in relation to the case study situation? Justify your answer with specific references to items within both the case study and the Codes themselves.

3) Problems of Advancing Technology (3 marks)

Nominate at least 3 other ethical/legal issues that you see potentially arising from the spread of the Internet and/or the rapid growth in technology. Explain why these are now, or could become, problems.

4) Report Professionalism and Communication (3 marks)

The report should be written as if meant for a professional audience and not just as an attempt to satisfy an academic course requirement. It should communicate clearly, exhibit attention to detail and present itself to a high standard, including:

- Good document structure including:
  - Title page (student name/number, tutor name, tutorial number, title, submission date);
  - Executive summary;
  - Table of contents;
  - Report introduction;
  - Numbered headings for each section;
  - Report conclusion;
  - Reference list page;
  - Additional appendices (if needed).

  Report should have numbered pages and good English expression (including punctuation and spelling). FEIT cover sheet should be placed at front of hardcopy submission.
- Clarity and insight - suitable word count (not counting title page, exec summary, toc, reference list, etc.) , deals properly with each topic without verbosity, shows a depth of analysis;
- Appropriate use of quotes, statistics and diagrams (where applicable) backed by properly cited sources. You need to cite at least **3** sources apart from those provided by the case examples. More are allowed if you wish. All references should be noted in the reference list at the end of your report and employ correct Harvard/UTS format;

Note for Repeating Students

If you previously attempted 31272 in **Spring 2015** then you may re-use your mark from that time in place of undertaking this assignment. If so, you MUST email the Subject Coordinator with your request by **5pm, 15 April 2016**. Return confirmation should be kept. Failure to obtain written approval by this time/date means the assignment is to be undertaken as normal.

Report Submission

Submission Requirements

Assignments are required in **BOTH hardcopy and softcopy**. Final-version hardcopy must be placed in the subject dropbox (CB11.05) by the due time/date nominated - with the corresponding softcopy submitted to Turnitin via the 'Assignments' tab of UTSOnline by the same time. Failure to provide a softcopy for plagiarism checking will be deemed an incomplete submission incurring a penalty of up to half of the assessment mark.

Marked hardcopies will be returned with feedback sheets by week 10.

Late Penalty

Late submission will attract a 2 mark per day penalty (including Saturday and Sunday). Submissions more than 5 days late receive zero unless special consideration has been sought from, and granted by, the Subject Co-ordinator prior to the due date.

Referencing Standards

All material derived from other works must be acknowledged and referenced appropriately using the Harvard/UTS Referencing Style. For more information see:

http://www.lib.uts.edu.au/help/referencing/harvard-uts-referencing-guide

Originality of Submitted Work

Students are reminded of the principles laid down in the "Statement of Good Practice and Ethics in Informal Assessment" (in the Faculty Handbook). Unless otherwise stated in a specific handout, all assessment tasks in this subject should be your own original work. Any collaboration with another student (or group) should be limited to those matters described in "Acceptable Behaviour" section of the Handbook. For essay questions, students should pay particular attention to the recognition of "Plagiarism" as described in that section of the Handbook. Any infringement by a student will be considered a breach of discipline and will be dealt with in accordance with Rules and By-Laws of the University. Penalties such as zero marks for assignments or subjects may be imposed.

Improve Your Academic and English Language Skills

HELPS (Higher Education Language and Presentation Support) Service provides assistance with English proficiency and academic language. Students needing to develop their written and/or spoken English can make use of the free services offered by HELPS, including academic language workshops, vacation courses, drop-in consultations, individual appointments and Conversations@UTS (www.ssu.uts.edu.au/helps). HELPS is located in Student Services on level 3 of building 1, City campus (phone 9514-2327).

The Faculty of Engineering and IT intranet (MyFEIT):
http://my.feit.uts.edu.au/myfeit)

and Faculty Student Guide:
http://my.feit.uts.edu.au/modules/myfeit/downloads/StudentGuide_Online.pdf

provide information about services and support available to students within the Faculty.

Useful Hints for This Assignment

1. ACS code of ethics and code of professional conduct can be found at:
   http://www.acs.org.au/about-the-acs/member-conduct-and-discipline
2. The **UTS Library on-line Journal Database** may help with your research. It is accessible from http://www.lib.uts.edu.au/databases/search_databases.py. You need to activate your UTS e-mail account (http://webmail.uts.edu.au/) in order access the resource.
3. The **Executive Summary** summarises the report's findings and recommendations. It can stand by itself as an overview of your ideas. Write it last. In contrast, an Introduction tells the reader what the report is going to cover.

Assignment 1 Case Study

Government will pay telcos and ISPs under metadata retention bill

By Daniel Hurst
(*The Guardian*, Thursday 30 October 2014)

http://www.theguardian.com/australia-news/2014/oct/30/metadata-retention-bill-will-require-data-to-be

Malcolm Turnbull introduces bill requiring data storage for two years, saying it is 'critical' to security agencies' operations

The bill will introduce a statutory obligation for telecommunications service providers to retain for two years telecommunications data. Photograph: Dave Hunt/AAP

The Abbott government will make "substantial" payments to Australian telcos and internet service providers under a new scheme requiring the companies to store data about their customers' activities for two years.

But the communications minister, Malcolm Turnbull, said he had no firm estimate of the cost of mandatory data retention, and argued the companies – not the government – were responsible for ensuring the safety of customer information.

Turnbull presented a bill to parliament on Thursday that would introduce "a statutory obligation for telecommunications service providers to retain for two years telecommunications data prescribed by regulations", saying it was "critical" for police and security agencies.

The Australian Federal Police (AFP) commissioner, Andrew Colvin, said access to the details known as metadata had application in a wide range of investigations, including pursuing illegal downloaders and file sharers.

The law will allow the storage of internet protocol (IP) addresses that were assigned to a customer and details of communications, such as the time, date, duration, sender or recipient, and phone numbers contacted.

In a bid to allay community concern over the storage of customer data, the government emphasised that the bill would not require a service provider to keep "the contents or substance of a communication", and nor would it require companies to store users' web-browsing history.

Turnbull said he expected "to make a substantial contribution" to the companies' implementation and operational costs, but the government did "not have a final figure at this point".

"We're asking these companies to do things that they don't have a business need to do and there is an expense," he said. "There are ballpark figures being thrown around but they are at this stage not of sufficient accuracy for me to be citing at the moment."

Labor has indicated it will consider its position, but the Greens warned the government to expect “a very serious campaign” against data retention. The Greens senator Scott Ludlam said the high costs were likely to be met through a combination of higher phone and internet bills and government taxes.

Ludlam said the government would “impose a surveillance tax on the entire Australian population and impose on industry an obligation that it doesn’t want, hasn’t sought, to track and store material on every device held by every man, woman and child in this country”.

The attorney general, George Brandis, said law enforcement agencies already could access metadata, but this depended on telecommunications providers storing the information of their own volition.

He said changing business practices and technology meant some metadata was no longer being stored, or would no longer be stored. Brandis argued a mandatory scheme was required to prevent “a very significant degradation of Australia’s counter-terrorism and general crime-fighting capabilities”.

The chief of the Australian Security Intelligence Organisation (Asio), Duncan Lewis, said access to metadata was critical to counter-terrorism, counter-espionage and foreign interference.

Colvin said metadata was important to national security operations but also “fundamental in most of the crimes, particularly serious and organised crimes, we investigate on a daily basis”. These included child exploitation cases, murders, physical assault and sexual assault.

“It is the tool we use often to place people at the scene of a crime or remove them from suspicion. It is the tool we use to help us refine what further intrusive matters or powers we may need to use down the track.”

Asked whether metadata could be used to target illegal downloads, Colvin said: “Absolutely. Any interface, any connection somebody has over the internet – we need to be able to identify the parties to that connection – not the content, not what might be passing down the internet. Illegal downloads, piracy, cyber crimes, cyber security – [in] all these matters, our ability to investigate them is absolutely pinned to our ability to retrieve and use metadata.”

Turnbull said securing the data safely was “the responsibility of the telcos and of course they’re very alert to data security already and very sophisticated in that regard”. He indicated the government was preparing separate legislation to strengthen telecommunications security.

Liberal and National MPs were told about the bill at a joint Coalition parties meeting on Thursday morning. The legislation will be referred to the parliamentary joint committee on intelligence and security for review. The timeframes for the inquiry are yet to be set.

The opposition leader, Bill Shorten, said Labor would carefully consider the legislation.

“We believe fundamentally in the promotion of national security,” Shorten said. “The security agencies say that they need metadata retained for two years. We balance against that the legitimate concerns for privacy. The good thing is that we have a parliamentary process and

parliamentary committees which will review these matters. We'll hear the evidence and calmly and rationally we'll make sure we get the balance right."

Ludlam said the Greens would stand up for the right to privacy, including the ability for journalists to talk to anonymous sources.

"At some point we have to draw a line. We are drawing the line at mandatory data retention," Ludlam said. "We've been warning the government for months not to cross this line. They have refused to listen to the evidence provided by civil society groups, by the telecommunications industry and by voices from across the political spectrum."

****

Edward Snowden lawyer: 'no evidence' data retention prevents terrorist attacks

By Shalailah Medhora
(The Guardian, Thursday 30 October 2014)

http://www.theguardian.com/australia-news/2014/oct/30/edward-snowden-lawyer-no-evidence-data-retention-prevents-terrorist-attacks

As Australian government introduces metadata retention bill, lawyer Ben Wizner says retaining data often impedes national security investigations

Edward Snowden's revelations about mass government surveillance turned public sentiment against data retention. Photograph: Guardian

The American lawyer for whistleblower Edward Snowden has questioned whether legislation to retain metadata will improve national security, as the Australian government introduces the bill to parliament.

Ben Wizner, a lawyer for the American Civil Liberties Union (ACLU) has told Guardian Australia that there's "no good evidence" that data retention aids national security authorities in preventing terror attacks.

"Having a massive database of records is unlikely to assist [law enforcement]. There is some argument that it does the opposite. That there's so many false leads that the FBI has stopped doing its traditional investigative work," Wizner said.

"Most plots are stopped not because of some fancy algorithm running through a database and forming connections, but because intelligence agencies have people undercover and they do old-fashioned police work."

He acknowledges that the retention of metadata can help connect the dots after an attack, but said: “I don’t think there’s a lot of evidence that mass surveillance is good at preventing terrorist attacks.”

The federal government introduced legislation forcing phone companies and internet service providers to retain users’ metadata – the digital footprint left behind when customers use their devices – for two years. That information would be freely available to law enforcement agencies.

In introducing the bill, the communications minister, Malcolm Turnbull, said it would not increase the extent to which metadata could be obtained by authorities. Rather, the bill established an industry-wide standard to make sure telecommunications companies kept this information for two years.

Both the prime minister, Tony Abbott, and the chief architect of the data retention bill, the attorney general, George Brandis, floundered in trying to explain what information would and would not be collected under the proposed legislation when they first floated it in August. Abbott’s office issued a statement at the time clarifying that web browsing history would not be included in data collected.

Tech experts and civil libertarians converged on parliament house on Wednesday before the bill was introduced to call on the government to release an exposure draft of the legislation that clearly defines metadata and explains what oversight provisions are in place to minimise the potential for data breaches.

“We have seen a significant history of data breaches in this country,” Narelle Clark from the Australian Communications Consumer Action Network said. “This kind of [retention] system will create a large honeypot with people who don’t have good intents and purposes.”

Chris Berg from the Institute of Public Affairs said the issue of who would bear the costs of the retention program were unclear but that it was likely they would ultimately trickle down to consumers in a “being spied upon tax”.

Jon Lawrence from Electronic Frontiers Australia was highly critical of the effect of the program on individual freedoms, labelling the bill “the single biggest threat to the liberty of Australians”.

The government has argued that data retention is necessary to protect the country from terrorist cells and lone wolf attacks.

“When it comes to counter-terrorism everyone needs to be part of Team Australia,” Abbott said in August.

“The highest priority of government is the safety of our community and I want to ensure the Australian people that we will leave no stone unturned to ensure that our community is as safe as it can be.”

The data retention policy, which is part of the third tranche of the government’s national security laws, has broad bipartisan support and is expected to pass through parliament.

Some crossbench senators have raised concerns over the bill.

“The idea that the government can watch all of us is fundamentally wrong,” Liberal Democrat senator David Leyonhjelm said on Wednesday, adding that authorities already had “plenty of existing powers” to deal with wrongdoers.

Public sentiment turned against data retention last year when Edward Snowden revealed the extent to which US security agencies were monitoring/storing phone and internet information.

While Wizner is against data retention, he acknowledges that the Australian government has handled the issue well, saying that the veil of secrecy often imposed by authorities on national security legislation is “deeply corrosive” to public trust.

A security expert for American thinktank the Brookings Institute, Benjamin Wittes, has told Guardian Australia that the Australian system of data retention is more effective than the US model which asked companies to “hang on to the data if they feel like it”.

“I think the ideal answer is a retention requirement for the companies themselves,” Wittes said, arguing that companies were less likely to misuse the data than government agencies.

****

A Guardian guide to your metadata

By Guardian US interactive team
(*The Guardian,* Thursday 13 June 2013)

http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1111111

(Edited by G. Mooney for 31272)

Metadata is information generated as you use technology, and its use has been the subject of controversy since NSA's secret surveillance program was revealed. Examples include the date and time you called somebody or the location from which you last accessed your email. The data collected generally does not contain personal or content-specific details, but rather transactional information about the user, the device and activities taking place. In some cases you can limit the information that is collected – by turning off location services on your cell phone for instance – but many times you cannot. Below, explore some of the data collected through activities you do every day:

Email

- sender's name, email and IP address
- recipient's name and email address
- server transfer information
- date, time and timezone
- unique identifier of email and related emails
- content type and encoding
- mail client login records with IP address
- mail client header formats
- priority and categories
- subject of email

- status of the email
- read receipt request

Phone

- phone number of every caller
- unique serial numbers of phones involved
- time of call
- duration of call
- location of each participant
- telephone calling card numbers

Camera

- photographer identification
- creation and modification date and time
- location where photo was taken
- details about a photo's contents
- copyright information
- camera make and model
- camera settings: shutter speed, f-stop, focal length and flash type
- photo dimensions, resolution and orientation

Facebook

- your name and profile bio information including birthday, hometown, work history and interests
- your username and unique identifier
- your subscriptions
- your location
- your device
- activity date, time and timezone
- your activities, likes, checkins and events

Twitter

- your name, location, language, profile bio information and url
- when you created your account
- your username and unique identifier
- tweet's location, date, time and timezone
- tweet's unique ID and ID of tweet replied to
- contributor IDs
- your follower, following and favorite count
- your verification status
- application sending the tweet

Google search

- your search queries
- results that appeared in searches
- pages you visit from search

Web browser

- your activity including pages you visit and when
- user data and possibly user login details with auto-fill features
- your IP address, internet service provider, device hardware details, operating system and browser version
- cookies and cached data from websites

****

Other interesting links to check

http://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152
http://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626