

Module Title: Professional Issues
 Exam Diet (April/Aug): April 2016
 Brief notes on answers:

1. Consider the following slide taken from a powerpoint presentation.

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS (TS//SI//NF) FAA702 Operations Two Types of Collection PRISM

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PaITalk, AOL, Skype, YouTube Apple.

You Should Use Both

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS (TS//SI//NF) Dates When PRISM Collection Began For Each Provider PRISM

Provider	Start Date
Microsoft	9/11/07
Yahoo	3/12/08
Google	1/14/09
Facebook	6/3/09
PalTalk	12/7/09
YouTube	9/24/10
Skype	2/6/11
AOL	3/31/11
Apple (added)	Oct 2012

PRISM Program Cost: ~ \$20M per year

TOP SECRET//SI//ORCON//NOFORN

a What organisation produced these slides? Why are they in the public domain?

The slides are part of an NSA presentation that was leaked by Edward Snowden.

b Critique the presentation of the slides. In what ways is it exemplary, and in what ways is it poor?

The information at the top is repeated on every slide, and wastes space rather than conveying new information.

The background map on the slide is obscured, and its relevance is unclear. The marks on the map are ugly and inaccurate. The logos copied onto the map are too small to read.

The 2-D layout is misleading, suggesting a linear relation between two variables. In fact, there is only one variable indicated, the horizontal timeline.

c “This slide deck would be improved if it made more use of bullet points.” Discuss.

Bullet points are unlikely to improve the presentation. Tufte explains that bullet points often lead to degradation of the level of argument, and in particular argues that poor presentation of slides, including bullet points, may be responsible for deaths in accidents with the space shuttle Challenger in 1986 and Columbia in 2003.

d The slides mention the FBI and Apple Computer. Describe a news story from 2016 involving these two parties.

The FBI has asked Apple Computer to disable security features of IOS that would allow it to unlock an iPhone belonging to Syed Farouk, one of the gunmen in the San Bernadino shooting that left 14 dead and 22 wounded. As of early March 2016, Apple Computer has refused.

2. The following definitions are adapted from the draft Investigatory Powers Bill, presented to parliament in November 2015.

- **Equipment interference** is access to electronic equipment such as computers and smartphones in order to obtain data, such as communications from a device. Equipment interference encompasses a wide range of activity from remote access to computers to downloading covertly the contents of a mobile phone during a search.
- **Communications data** is information about communications: the who, where, when, how and with whom of a communication but not what was written or said. It includes information such as the subscriber to a telephone service or an itemised bill.

Explain how equipment interference and access to communications data are regulated under current legislation? *Marks will be awarded for mention of specific acts and issues – examples listed below are not exhaustive.*

Your answer should include consideration of the following questions:

- What risks do these activities pose to individuals and corporations? *Various, including, e.g. invasion of privacy, identity theft, financial loss, IP theft, unfair competition.*

- How does the law protect them from these risks? *Computer Misuse Act: Unauthorised access to computer material, Unauthorised access with intent to commit or facilitate a crime, Unauthorised modification of computer material, Making, supplying or obtaining anything which can be used in computer misuse offences. Data protection act: eight data protection principles. RIPA: unlawful interception.*
- What sanctions are there for unauthorised equipment interference and unauthorised access to communications data? *Computer Misuse Act: up to 5 years imprisonment, unlimited fine. Data protection Act: unlimited fines. RIPA: unlawful interception – two years imprisonment.*
- What provisions exist to enable authorised equipment interference and access to communications data? *Codes of practice: data retention – for a wide range of purposes, including health, tax, emergency, safety, crime, security; authorised interference by the Intelligence Services, or persons acting on their behalf or in their support; Interception in accordance with a warrant issued under section 5 of RIPA (to Police, Intelligence and Security services).*

It should briefly discuss any conflicts and additional risks associated with legislation of these activities. *Qualified right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. Intelligence Services must act proportionately. Risks of backdoors, risks of unauthorised access to retained data, risks of misuse by authorised persons.*

3. The following story appeared in the Sunday Herald in March 2015.

The UK’s privacy watchdog has warned that plans to create a “super ID database” may lead to the creation of a national identity number for every Scot by default.

In what critics claim is a devastating blow to SNP proposals, the head of the Information Commissioner’s Office in Scotland has called “suitable safeguards” to be put in place for the plan to give more than 100 public bodies the right to request access to an NHS database containing private information about individuals.

Under the proposals, access would be granted to the HMRC, which would use the information to help build up an accurate database of Scottish residents ahead of the devolution of powers over income tax to Holyrood.

Other bodies that would be entitled to request access to records and update the database include the police, airports, Quality Meat Scotland and Scottish Canals.

a What UK legislation is relevant to the above proposal?

UK Data Protection Act of 1998.

b Name two data protection principles relevant to the proposal, and explain why they are relevant.

The third and seventh principles are particularly relevant. Arguably, in this case the data collected is excessive, and making it available to so many organisations subjects it to inappropriate use.

First data protection principle: Data subject must give consent.

Second data protection principle: Data must be collected for specified and lawful purposes.

Third data protection principle: Personal data shall not be excessive in relation to the purposes for which collected.

Fourth data protection principle: Data must be accurate and kept up to date.

Fifth data protection principle: Personal data shall not be kept longer than is necessary.

Sixth data protection principle: Personal data shall be processed in accord with the rights of data subjects.

Seventh data protection principle: Appropriate technical and organisational measures shall be taken against inappropriate use.

Eighth data protection principle: Personal data shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the rights of data subjects.

- c The Identity Management and Privacy Principles, published by the Scottish Government in October 2014, states in Section 4.6:

“If a public service organisation needs to link personal information from different systems and databases (internally or between organisations), it should avoid sharing persistent identifiers; other mechanisms, such as matching, should be considered.”

Explain how this impacts on the above proposal.

The plan is to link many different databases together with a universal identifier (UCRN), which is what results in a so-called “super database”. The guidelines suggest it would be better to use matching (say, on name, birthdate, and address) rather than a UCRN.

- d What might be the impact on data protection if the UK votes in the upcoming referendum to leave the EU?

European Convention on Human Rights guarantees right to privacy in Section 8.1.

UK Data Protection Act was a response to a Council of Europe Convention on data protection.

Rulings of EU court impact on data protection, e.g., the recent ruling that the US no longer counts as a “safe harbour” for data.