P1 2017

1. You work for a mobile software company.

   a. 2 aspects of BCS for tracking information.

   - public interest - wide-reaching collection of personal data.
   - duty to relevant authority - public interest issue here and this may lead to conflict between your professional obligations and DPA.

   b. 3 Questions to ask the company wrt legal operation of company.

   - how do we handle issues of consent? → breach of DPA
   - any way of managing where data is exported to from the software? Concerns of data moving to less well-protected environment.
   - how long is the data retained? (should not be unlimited)

   c. 2 aspects of GDPR that impacts this.

   - data portability requirements might pose significant issues because the system may integrate many individuals activity.
     - giving the data back to the users
   - explainability of the algorithms that decide on what ads to show may also be difficult to explain to a non-technical person.

   d. Two ethical principles that are important.

   - privacy - personal data should not be released to third parties w/o consent.
     → ensure trust in system
   - transparency - clear information flows + how information contributes to choice of other actions.
     → underpins the ability to explain the operation of the system

2. Internet surveillance by Police and government.

a. Issues to the communication campaign.

- information on sorts of crimes the act is trying to prevent
  e.g. drug trafficking, money laundering
  - need to retain info for a long time to get patterns

- pattern of comms is more important than the content
  - rare for security organisations to look into private information

- most of the data is not involved in investigations because it is not relevant.
  - loss of liberty vs. gains in controlling criminal behaviour

b. Balancing perspective that looks at the wider consequences of such legislation.

- how strong is the evidence that this works?
  - few concrete evidence that this works
  - need more accountable framework for surveillance so we can judge effectiveness.
  - often information comes from whistleblowers / insider info.

- security org'ns are opposed to strong encryption on message contents
  - not just to see patterns?

- what if the structure of state changes to more authoritarian?
  - dismantled presumptions of privacy

c. Why is surveillance ineffective towards organised crime and other national states?

- corruption - pay key individuals money to avoid capture
  - can be organisations gathering the data / in those that interpret the data.

- technical competence - many nations have highly competent cyber ops units associated w/ military and security
  - hard to detect.

3. Public sector, NHS, social care

a. Organisational structure of these public bodies

- bureaucratic
  - managing large delivery organisation
  - clear lines of responsibility
  - clear routes to promotion to incentivise capable people

b. Issues of merging these organisations

- difficulties around crossing line management responsibilities
  - there needs to be a senior to adjugate conflicts
  - we are pulling two different hierarchies → conflict

- performance judged by diff. metrics
  health: successful procedures
  care: softer issues (good Q housing)
  } combine metrics

- who will be responsible to combine organisations?

c. Decision-making algorithm.

i. Two main challenges

- how to introduce the approach into already established processes - resistance from workers, fear of job loss, etc.

- how to capture the decision process, get adequate data to validate the decision support system.

ii. Unintended consequences

- if the decision support system generates more decisions requiring action this could stress services.

- algorithms might be biased → discriminate against some group or individual.