Solution Notes for COB201 Exam Revision Questions

Q1

Please see the Just-Eat Privacy Policy or Deliveroo Privacy Policy in detail.

See the summary below.

Information that you provide voluntarily:

Registration information when you create an account

Transaction Information when you place an Order with a Restaurant

Information regarding your marketing preferences so we can:

Feedback on your views of Services

Information collected automatically

Activity Information: information about customer usage of the Services and information about themselves from the content they create and the notifications or messages they post or send as well as what they search for, look at and engage with

Cookies and similar technologies (e.g. your Internet Protocol (IP) address, your device ID, your browser type and when, how often and how long you interact with the Services)

Information obtained from third-party sources

Analytics reports and market research surveys: information from the third-party affiliates about the way customer respond to and engage with their marketing campaigns

aggregated information in the form of audience segments from third party sources in order to display targeted advertising on digital properties operated by organisations like Facebook and Google.

Q2

See Sensitive personal data /special category data on the ICO website.

Important part is data matching and finding patterns of a specific activity. For example, a customer always places much more pizza orders on St Patrick days. St Patrick day is observed by the Catholic Church and that information is publicly available.

Q3

Note that one question can be answered using what you learned in all the module , here using the code of conduct and ethics, as well as the computer misuse act. Like the “Rogue use case”, hacking is illegal, but here it was in the purpose of “avoiding Harm”

What solution does a Kantian approach (Deontological Ethics) offer?

In this Kantian approach we have to ask 'what would happen if everyone did it? this is, can it be universalised we have to decide whether this is hacking. If it is (which it certainly looks like she will be accessing illegally someone else’s network), then she would be morally wrong in hacking the system. There is no provision in the Kantian terms for accessing something owned by someone else without permission. In other words, it does not matter that the third-party are bad people

What solution does a consequentialist approach (Utilitarian Ethics) offer?

The consequentalist position would look for the greatest benefit to the great number of people. We could say that the population and the environment of the targeted country would be harmed and therefore, whether the programmer is hacking or not it would be a morally right thing to do. However, we have also to take into consideration the large number of organisations and the beneficiaries, who are the greater in the number.

Are their conclusions the same?

This depends on certain factors whether she is hacking (Kantian) or how we calculate the benefits of the largest number (population of the targeted country versus advertisers and beneficiaries). If this is not hacking then the outcome is good. If it is hacking then Kant would say no. if the population is the greater good then consequentialism would say yes.

What do you think she should do and why ?

If this hacking action might be detected by authorities, Rebecca’s team could put a proposition to the relevant authorities that they could use hacking ethically in a good cause this would benefit them from a public relations perspective. if she would be hacking the target even after the missile is stopped, our answer would be that she should do this regardless of the numbers of the population versus the beneficiaries of the company. It seems then, that we hold on consequentialist position.

Q4

See the lecture- Cyber security and Hacking (week 6)

COB201 – Professional issues in computing

Q5

See the lecture- Cyber security and Hacking (Week 6)

Section 1: Unauthorised access to computer material

Section 2: Unauthorised access to computer material with the intent to commit orfacilitate further offences

Section 3: Unauthorised acts with intent to impair, or with recklessness as toimpairing, operation of computer.

Q6

See the lecture slides in Week 5 and DPA 2018 Principles on ICO

Principal: 1) Purpose limitation and 2) lawfulness, fairness and transparency

A brief explanation required.

Q7

See the lecture slides in Week 5 and DPA 2018 Accountability on ICO

1. Make it compulsory for every member of staff in the call centre to attend the council’s DPA training.
2. Enter into a legally binding agreement with the call centre that guarantees compliance with the DPA.
3. Ensure that the breach management process is part of the agreement, in order to support the council in complying with the deadline of 72 hours to report a personal data breach.

Q8

Please see the solution below which is from Page 95 of the book- Ethical, legal and professional issues in Computing (Duquenoy, jones and Blendell).

Free speech is a basic human right, and one of the key, underlying principles of open, democratic society. Genuine debate and criticism is necessary in any political process, to test assumptions, and expose false ideas, and to enable people to choose their political representatives freely. Censorship can lead to the suppression of opposition, the loss of freedom, and ultimately, totalitarianism (as in Nazi Germany or the Soviet Union).

Q9

See the lecture slides- freedom of expression in Week 9.
"…the suppression or regulation of speech (in its broadest definition) that is considered immoral, heretical, subversive, libellous, damaging to state security, or otherwise offensive. It is the control and regulation both of what people can and cannot say or express, and what they are permitted to see, read and view." Duquenoy et al, p.81-82.

In general, Censorship is justifiable when something is offensive to the majority of the population. Anything that strives to incite hate or violence should be censored as well.

Q10

See the lecture slides- freedom of information in Week 9.

To create transparency within government and make public authorities accountable to the public.

Q11

See the lecture slides- freedom of information in Week 9.

- Information relating to national security, law enforcement, commercial interests and personal data
- Test of prejudice – for example, release would prejudice the prevention or detection of crime, OR
- Public interest test – public interest in withholding it is greater than the public interest in releasing it.
- Information which is 'readily accessible' elsewhere / in another format
- Information intended for future publication
- Information that, if disclosed, would be likely to prejudice UK international relations or interests
- Information that, if disclosed, would be likely to prejudice UK economic or financial interests
- Ongoing criminal investigations
- Vexatious or repeated requests.

Q12

Dominos would wish to know the events in advance so that they could be better prepared or marketing appropriately.

Write to Lboro University and find out the planned events

Please see the FOI requests on the link:
https://www.whatdotheyknow.com/list/successful

Q13

See the lecture slides- Cyber security and Hacking in Week 6.
A large number of computers are set up to send a large number of requests to a particular server at a particular time and make a service unavailable or too slow for the legitimate users.

Firewalls and IDS could be utilized and be configured to protect from a DDOS attack. Firewall and IDS are used to scan and filter suspicious traffic.

Q14

See the lecture slides- Cyber security and Hacking in Week 6.

Network scanners check for vulnerabilities on your own system (e.g. open ports, accounts without passwords) but some can also check for vulnerabilities from outside the system in order to explain them and launch an attack.

See the detailed discussion on Review.

Q15

See the lecture slides- Copyright in Week 3.

Idea, algorithms and mathematical formulae

Q16

See the lecture slides- Copyright in Week 3.

Database is owned by the maker of the database. If they are employed, then it is owned by their employer. Database right stops people copying a significant amount of information from that database and using it for their own purposes.

Software used in the making or operation of a database is specifically excluded from protection as a database, instead it is generally protected by copyright as a literary work.

Q17

Deduced from lecture ‘computers in the workplace’ Week 10

1. checking phone logs
2. checking logs of websites visited
3. recording on CCTV cameras

Q18

Name the act that applies to each of the following statements:

Statement	**Act**
Part of the data stored in health clinic servers have been shared with a third party company without the clients knowledge	**Data protection Act**
Someone hacked into the clinic databases and accessed confidential data	Computer misuse Act
The clinic informed all the users having data stored on the hacked database	Computer misuse Act
The clinic accepted to comply with any request of information they hold, according to their publication scheme.	Freedom of information Act

Q19

Below is a list of key areas that apply to Data Governance.
In the following table, indicate the Key Area that applies to each statement.
List of key areas.

- Retention Management (RM)
- Records Management (RecM)
- Defensible Disposal (DD)
- Information Storage (IS)
- Social Media (SM)

Statement	**Key area**
Eliminate irrelevant or duplicate data	DD
Data categorisation is important to help in data management	RecM
Identify emerging and new technologies that might be deployed to increase business benefit	IS
Data is kept for a specific period of time; a policy will dictate what to do the period expires	RM