

## Quiz questions 2008 – answer sheet

1. What year did the Privacy Act come into force?

- (a) 1984
- (b) 1989
- (c) 1993
- (d) 1996

*Answer: (c) – 1993*

2. Requests for access to information have to be in writing. True/False?

*Answer: False. It may be more administratively convenient to ask for an access request to be put in writing, but even an oral request is still a valid access request and is subject to the same procedural requirements. Note the agency's obligations under section 38 to provide the requester with assistance – this might extend to helping the person fill in a request form.*

3. How many working days do you have to respond to a request for access to information under the Privacy Act?

- (a) 7 or earlier if possible
- (b) 10 or earlier if possible
- (c) 20 or earlier if possible
- (d) 30 or earlier if possible

*Answer: (c). 20 working days is the maximum (unless an extension is required – see section 41), but the decision on the request should be made “as soon as reasonably practicable”.*

4. How soon do you have to provide information in response to a request for access under the Privacy Act?

- (a) 10 days
- (b) 20 days
- (c) 30 days
- (d) Without undue delay

*Answer: (d). Section 66(4) says that information must be provided without undue delay. If there is undue delay, this is a deemed refusal to provide the information which may then lead to an interference with privacy (section 66(2)).*

5. Which of these are *not* grounds for withholding information that a person has requested under the Privacy Act? (there are multiple answers)

- (a) that disclosure would prejudice the commercial position of the person who supplied it
- (b) disclosure would breach a promise of confidentiality
- (c) disclosure would impede free and frank discussion between officials
- (d) disclosure would breach legal professional privilege
- (e) disclosure would prejudice the security of Tokelau

- (f) disclosure would cause political embarrassment
- (g) disclosure would reveal the identity of an informant

*Answer: (b), (c) and (f). (f) is simply not a withholding ground. (c) is similar to a withholding ground in the Official Information Act, but does not feature in the Privacy Act. (b) is a trick – information has to be **both** evaluative material **and** subject to a promise (express or implied) of confidentiality before the withholding ground (section 29(1)(b)) will apply. This is a common mistake.*

6. Does the law require an agency to have a Privacy Officer? Yes/No

*Answer: Yes. Section 23 of the Act requires an agency to have a privacy officer.*

7. Can you name other countries in which there is data protection legislation like New Zealand's Privacy Act?

*Possible answers include: Australia (federal and in several states), the UK, Canada (federal and at provincial level), Hong Kong.*

8. How many Privacy Commissioners have there been in New Zealand?

- (a) 1
- (b) 2
- (c) 3
- (d) 4

*Answer: 2 [if you don't count the Wanganui Computer Centre Privacy Commissioner!]*

9. If an employee of an agency breaches the Privacy Act, it is the agency that takes the blame, not the employee. True/False?

*False – strictly speaking. The agency certainly generally carries the responsibility (see sections 3 and 4) but the employee may also be personally liable, for example if the agency can put forward a defence under section 126(4) that it did everything that it could reasonably do to prevent the breach from occurring.*

10. When you collect personal information from someone, you have to make sure that that person is aware of certain things. Which of the following is *not* one of those things?

- (a) why you need the information
- (b) how long you will keep the information for
- (c) who you might disclose the information to
- (d) what will happen if the person doesn't give you the information
- (e) what statute requires you to collect the information (if relevant)

*Answer: (b).*

11. Principle 5 (storage and security of personal information) requires an agency to train its staff in how to handle personal information. True/False?

*Answer: True. While principle 5 does not say this explicitly, training staff is part and parcel of ensuring that information is kept secure. An early Tribunal case (*W v Director-**

*General of Social Welfare (CRT Decision 11/98, 12/98; (1998) 5 HRNZ 580) reinforces this view.*

12. If a journalist rings and asks for information about one of the agency's clients, you need to make sure that principle 11 (disclosure) allows you to reveal that information. True/False?

*Answer: It depends(!) - on whether the agency is a public sector or private sector body. If it is a public sector body, the Official Information Act governs whether the journalist should receive the information. Principle 11 is not directly relevant (though it might help you to gauge how strong the privacy interests actually are in that situation).*

*If the agency is a private sector agency, then principle 11 of the Privacy Act may well be relevant.*

13. Generally, you should not use or disclose personal information except when this is the purpose for which the agency has got that information. However, there are exceptions. Which of the following is *not* an exception to that rule:
- (a) the individual concerned has authorised the use or the disclosure of the information
  - (b) another statute requires you to use the information in this way, or disclose it
  - (c) the agency has entered a contract with a third party which requires the use or disclosure of the information
  - (d) the use or disclosure is necessary because there is a serious and imminent threat to someone's safety

*Answer: (c).*

14. Agencies should not collect personal information unless:

- (a) the information is needed for a lawful purpose
- (b) the information is needed for a purpose that is directly related to the function or activity of the agency
- (c) the information is collected lawfully, and by means that are fair and not unnecessarily intrusive
- (d) either (a) or (c) as long as one applies
- (e) either (b) or (c) applies
- (f) both (a) and (b) apply but not (c)
- (g) (a), (b) and (c) all apply

*Answer: (g). An agency collecting personal information needs to comply **both** with principle 1 [covering (a) and (b)] **and** principle 4 [covering (c)].*

15. If an agency corrects personal information, when the person asks it to do so, the agency does not have to do anything else. True/False?

*Answer: False. Principle 7(4) states that an agency that has corrected information, or attached a statement of correction, must – if reasonably practicable – inform each person, body or agency to whom the personal information has been disclosed that it has been corrected, and what the correct information (or statement of correction) is. This ensures that everyone in the information chain has the same 'correct' information to work from.*

16. There is only an interference with privacy if the person concerned can show they suffered harm as a result of a breach of a privacy principle, rule of a code of practice or information matching provision. True/False?

*Answer: False. Most breaches require the complainant to demonstrate that they have suffered harm as a result – or that they may suffer some reasonably definite harm in the future (section 66(1)). But a refusal to give access to information on request is an interference with privacy unless there is a proper basis for that refusal (section 66(2)). The same is true of a refusal to correct, a breach of section 40, or undue delay in providing access to the information (section 66(2),(3) and (4)).*

17. Which of these is not a unique identifier?

- (a) IRD number
- (b) PIN number
- (c) Student ID number
- (d) NHI

*Answer: (b).*

18. Which one of the following statements is *not* correct? Authorised information matching programmes can only operate when:

- (a) there are 10 or more records to be matched at a time
- (b) there is legislation authorising the match to be done
- (c) the purpose is to produce or verify information about individuals
- (d) the results of the programme are regularly reported to the Privacy Commissioner

*Answer: (a). There is a common misconception that there cannot be an authorised information match until the magic number of 10 records is reached. But this is not the case. The number 10 is a useful trigger for considering whether an authorised match is really needed – with the possible logistical difficulties of passing enabling legislation etc. It is not a requirement, though, for the programme to be an authorised match.*

19. If information is on the database, you never need to check its accuracy before using it. True/False?

*Answer: False. Principle 8 says you need to take reasonable steps to ensure that information is accurate – and relevant, up to date and not misleading – before you use it. What will be reasonable will depend on the circumstances. It is not necessarily reasonable simply to rely on the record that you happen to have.*

20. Most complaints to the Privacy Commissioner in 2006/07 were about:

- (a) disclosure of personal information
- (b) access to personal information
- (c) accuracy of personal information
- (d) surveillance

*Answer: (b) – around 40% of complaints are about access to personal information under principle 6.*