UNIVERSITY OF CAMBRIDGE
DEPARTMENT OF HISTORY AND PHILOSOPHY OF SCIENCE
Free School Lane
Cambridge CB2 3RH U.K.

Richard C. Jennings
Tel: Cambridge (01223) 334540/1
Fax: Cambridge (01223) 334554
e-mail: rcj11@cam.ac.uk

7 May 1999

Dr D J Greaves
Computer Laboratory
Pembroke Street
Cambridge CB2 3QG

Dear Dr Greaves,

Professional Practice and Ethics lectures

Following are the two questions I suggested for Paper 2 of the Part IA Computer Science Tripos 1999 exam along with ~~ideal~~ model answers. The ~~ideal~~ model answers are taken more or less directly from my distributed lecture notes.

20 mark question:
What is the nature of privacy and how do EU guidelines and/or British legislation serve to protect privacy?

A. Personal privacy - what is it?

> [Of the following, points 1 to 3 may appear since I discussed them, but the crucial points are 4 and 5 - especially point 5. However a good argument supporting a different position, or against the position of point 5 (or 4) should be given good marks for that part of the answer]

1. Secrecy?
Because in some situations privacy involves withholding information about ourselves, we may be tempted to think that secrecy is an essential feature of privacy. But secrecy involves actively withholding information and privacy may simply involve retaining information. We do not tell everyone everything about ourselves, that would be boring. But neither do we regard all that information as secret. Just because information is private does not mean it is secret. Nor is secret information necessarily private. We may be party to state secrets, or to business secrets, that are shared by a large number of people. These secrets are not private, but they are nonetheless secrets. Secrecy and privacy overlap when they require conscious supression or hiding of information, but we can have secrets that are not private and we can be private about things that are not secret.

2. Anonymity?
One suggestion about privacy is that it consists in anonymity - as long as we are not known by name any information about us will not affect us, thus our privacy is preserved. But our names are only of use if there is a databank which connects information with our names. And anyway

we wouldn't share some information even if we remained nameless. Maintaining anonymity may be a way of maintaining privacy, but it is not the same.

3. The private vs. the public sphere

Another idea about privacy is that it is a characteristic of certain kinds of information about us, it assumes that there is a sphere of private knowledge and a sphere of public knowledge. So, for example, our name, our sex, our accent, and so on, are part of the public sphere while our sexual inclinations are part of the private sphere. If we think about it there is virtually nothing about us that is not known by someone in our lives. But one important feature of this fact is that we know in general who knows what about us. Privacy is not so much a personal matter as a matter of social relations.

4. Privacy as control of personal information

In 1978 the British government Lindop Committee reported on their investigations into the field of data protection and as part of that considered the question of data privacy. For them the concept of data privacy referred to the individual's claim to control the circulation of data about himself. But information about me can circulate in normal and non-invasive ways without my control. The sharing of the information is partly controlled by the individual, but much of it is not. Privacy is preserved as long as it is distributed in legitimate ways along legitimate channels of social relations.

5. Privacy: an aspect of social relations

It seems paradoxical to think of privacy as an aspect of social relations. But we have seen that nearly everything about us is, or could, be known by someone. It is just that some things are appropriately known by some people, and other things appropriately known by other people. The sort of thing that is appropriate for a person to know depends on the kind of relation they bear to us, the role they play in our lives. A person's privacy does not consist in a particular batch of information (the private sphere) that they keep to themselves, nor does it consist in being in total control over the distribution of information about themselves. Rather it consists in that information being appropriately distributed over the network of social relations in which that person is involved. Privacy is violated when information is distributed in a way that is not appropriate to those social relations.

B. How can we protect privacy?

> [This is a more philosophical introduction to the following section on privacy legislation. I do not feel it is essential to the answer, so candidates should not lose points for its absence, though they should be given points for its appearance.]

If privacy is violated when personal information is distributed through inappropriate channels, then what principles should we adopt to prevent this? One principle we could adopt is that:

1. The recipient of personal information must have a legitimate use for it.

This principle limits the collection of information to what is appropriate to the circumstances. The concept of legitimate use for information plays an important part in this principle. We need to state more explicitly what it is to have a legitimate use for information. This is done by a second principle:

2. The purposes of the recipient in acquiring the information must be connected in a positive way with the interests of the subject of that information.

In other words we should consider whether the subject of the information would want to have the information passed along to the recipient. Now obviously some such transfers of information are not in the interests of the individual, but still serve some greater interests. The

criminal does not have a right to privacy about his criminal activities because he does not have a right to act criminally. However, there is a balance that needs to be maintained here. The police cannot be allowed free and easy access to all information on everyone. There must be some limits on their powers to access confidential files, just as they have some rights to access files. The fact that different files have different degrees of confidentiality suggests a third principle to maintain the balance:

3. The availability of personal information must be inversely related to the degree of confidentiality under which it was originally obtained.

And finally, as a control on the distribution of data, a way of ensuring that the second principle is maintained, we can adopt a fourth principle:

4. The subject must have some practicable means of discovering what information about him or her has been transmitted to whom, and must have access to it.

These principles are aimed at preserving the right of privacy in a world where information can easily be gathered, stored and transmitted. They do not preserve an absolute right to privacy, but they assume the right in the absence of some overriding factor. Justification is needed for the acquisition of information, not for the protection of it. The assumption is that information should not be transmitted unless there is good reason to do so.

C. Official Guidelines and Legislation

> [This is an essential section, though it is long and the candidate would not be expected to cover the whole ground in detail. What is important is that what s/he does cover is related to the first part of the question - the candidate should be able to explain how the legislation serves to protect privacy as they have described it in the first part of the question. Alternatively, if the candidate offers a contrary, or deviant argument, that should be assessed on its own merits - e.g., if someone argues that privacy is other than I have argued above and goes on to show that the following legislation does not protect privacy in their sense (showing good knowledge of the legislation) then I can imagine giving them good, even full, marks.]

Having arrived at some moral principles, we can now look at privacy legislation and see how these principles are implemented. In 1980 the Organization for Economic Co-operation and Development (OECD) published *Guidelines on the Protection and Privacy of Transborder Flows of Personal Data.* The guidelines set out eight principles for the protection of privacy in data collection, handeling and distribution. The guidelines were adopted by all 24 OECD member countries and provided the foundation for the United Kingdom Data Protection Act of 1984, the "DPA". The DPA of 1984 is due to be superseded in January 1999 by the DPA of 1998, which is intended to bring UK legislation into closer alignment with European legislation. Currently registered personal data processors will be allowed a transitional period of up to two years to bring their operations in line with the European principles. The following are the eight principles of the 1998 DPA. Most of the principles are self explanatory, but the first and sixth principles require some unpacking.

1. First Principle:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The basic condition for a) is that the subject has given consent for their data to be

processed, but there are a number of exceptions such as processing that is required for performance of a contract to which the subject is party, and processing that is required by the government. The "sensitive personal data" of clause b) includes data on such things as the racial or ethnic origin of the data subject, their political opinions, their religious (or similar) beliefs, their sexual life, and their criminal record.

Under the DPA of 1998 the subject must at least actively consent to having personal data gathered (e.g., failure to return or respond to a leaflet does not count as consent) and where the data is more sensitive they must explicitly consent to having the data processed (i.e., write it down).

The First Principle also subsumes two other important aspects of personal control of data - the right of the data subject to know what personal data is being gathered (the old OECD openness principle) and the uses to which that data is being put (the old OECD purpose specification principle).

The OECD purpose specification principle appeared as principle 2 of the UK DPA of 1984. In the DPA of 1998, purpose specification is included in the principle of fair and lawful processing. In particular, this first principle contains a fair processing code which specifies the information to be provided to data subjects. In addition to the identity of the data controller, the data subject must be told the purpose for which the data are to be processed. But the requirements do not stop here - the data subject must also be informed of the likely consequences of such processing and especially whether disclosure of such information can reasonably be envisaged. In particular the data processor is obliged to inform the subject of consequences of processing that the subject may not forsee.

The OECD openness principle held that the data subject should be able to determine the whereabouts, use and purpose of personal data relating to them. The availability of this kind of information creates its own problems of security. We can imagine files which hold personal data about individuals who do not object to having that data held, but who would object to other people knowing that that data is held. For example, police records, or hospital records of people who are HIV positive, or building society records of people who have had to renegotiate their mortgages because of financial hardship. In such cases it would be a breach of privacy if someone else could discover the whereabouts, use and purpose of personal data relating to them. A central register of individuals and the files which included them would then itself require a high degree of security and pose a potential threat to privacy. For this reason no central register is kept, and the openness principle is reduced to the rights of data subjects covered by the sixth principle.

2. Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purposes or purposes for which they are processed.

4. Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

5. Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The first right of the data subject is to be told by any data processor if their own personal data is being processed and, if it is, to be told in an intelligible manner what that personal data is, the purposes for which it is being processed, and to whom the personal data may be disclosed.

The data subject also has the right to prevent processing for purposes of direct marketing or where the processing is likely to cause damage or distress, and the data subject has the right to seek a court order requiring the data controller to rectify, block, erase or destroy inaccurate data.

Finally, the data subject has the right to seek compensation for any damage or distress that may result from contravention of the act.

7. Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The act is enforced through the office of the Data Protection Registrar (DPR) who maintains a register of data collectors and processors. Individuals and organizations who regularly process personal data are legally obliged to register themselves with the DPR. They must state what kind of data they are processing and for what purpose they are using it. They are breaking the terms of the DPA if they use the data for any other purpose than what is stated. In addition to the penalties that may have to be paid to individuals if damage is done through misuse of personal data, the data processor can be struck off the register of data collectors and processors. If he is struck off the record then it is illegal for him to store or process any electronic personal data.