UK REGISTRAR EXPLICITLY ADDRESSES PRIVACY ISSUES

The UK Data Protection Registrar's Eighth Annual Report, published in July 1992, has reached out more clearly than ever before beyond narrow data protection concerns to specifically address privacy issues. The Registrar's conclusion to his report states that "without adequate protection there is a grave danger that individual privacy will simply be whittled away." Dr. John Woulds, Senior Assistant Registrar, explains.

The challenge to individuals' privacy comes from both a drive for administrative efficiency and technological innovation, for example:

Census Office Register: The Census Office is looking at different ways to carry out censuses by using data that is collected for other administrative purposes, and then extract from those databases the information they need to form a national population register. This idea may never be put into practice but illustrates the kind of pressure the Data Protection Office is put under.

Telecoms Technology: The technological advances in telecommunications pose a risk to individuals and Calling Line Identification (known in the US as Caller ID), raises important issues for the DPR.

Document Image Processing: Document image processing systems hold personal data in a way which poses rather difficult questions on interpretation of the legislation.

Such changes over the last two decades pose risks to individual privacy. The Council of Europe Data Protection Convention sought to draw a certain balance between the rights of individuals and other public objectives. The UK Data Protection Act, which was enacted to allow the United Kingdom to ratify the Council of Europe Convention, does not deal explicitly with the issue of privacy. Nevertheless, it does establish rights for individuals and recognises that those rights should be set against other objectives.

The DPR's office is active and has made progress and achieved some success in virtually every area of life involving personal data.

Direct Marketing

There is an increasing acceptance by direct marketeers of the requirements of the first Data Protection principle; fair collection of personal data, meaning that people should know when they give information who is going to use it, and to whom it is to be disclosed. Standards are being adopted to meet this principle when information is collected for marketing purposes. The notification given to the individual and the opt out or check off box is seen as a very helpful option from the data protection point of view. The individual states that he does not wish to see the information given by him being used for a different purpose than the one for which it has been collected.

It is also helpful to see the rules for direct marketing, including principles of database management, that have been adopted by the Advertising Standards Authorities as an extension to the scope of the British Code of Advertising Practice. There are strong statements in those rules such as the requirement that obtaining, compilation, processing and management of data should conform with the data protection principles. Furthermore, the rules support the views of the Registrar on the fair collection of personal data. Such moves were welcomed by the DPR.

The Council Tax

A second front of progress is in relation to the Council Tax, the new system of local taxation that is being introduced by the UK government with effect from 1 April 1993. The council tax is a property based tax, but it does have some personal information associated with it. For instance the liability to pay the tax will fall on individuals, and there are provisions for discounts for single occupant households, meaning that personal data will be involved in the management of the tax. There is a need to use valuation lists of properties as the basis for the council tax, and the government is taking the view that such lists

should not be available for commercial sale, for instance, for enhancing housing databases or for direct marketing purposes.

In relation to such personal data, some issues that arose with the previous tax, the poll tax, also apply, for example, fair obtaining of data, holding data not relevant to the purpose for which it has been collected, not holding data for longer then needed, etc. Such issues caused a lot of problems to the local authorities and to the DPR and it is hoped that such problems will not arise again. The Department of Environment is preparing practical guidance on data protection and the council tax, and the Registrar's office is working closely with both the Department and the Local Authority Association to avoid those earlier problems.

Purchase of Electoral Registers

Ministers this year have agreed to introduce a scheme to encourage electoral registration officers to list those organisations which have bought copies of the register and their reasons for purchasing them. These lists will be available for inspection by the public, which enables individuals to trace who has purchased information about them.

Vehicle Inspectorate

The Vehicle Inspectorate maintains records for goods vehicle operators and is often under pressure to make further use of the information collected, and if possible make a profit. The Inspectorate has agreed that it will give appropriate notification to both existing and new operators on their lists, and also give them the opportunity to opt out of any commercial use of the information that is supplied. This is very interesting because such information is collected under statutory provisions and therefore does not fall under the Data Protection Act. Nevertheless, the Inspectorate agreed to this proceeding even though it has no legal obligation to do so.

Credit Reference Agencies

There has been a long running dispute between the Registrar and the credit reference industry on the use of third party information for assessing credit. The Registrar issued enforcement notices against the four main credit reference agencies some time ago which required them to stop extracting information about a third party not associated with the applicant for credit. The agencies appealed to the Data Protection Tribunal and the Tribunal revised the Enforcement notices issued by the Registrar. The Tribunal supported the Registrar's point of view that extracting information on people that never lived with the applicant for credit is unfair processing under the DPA. Therefore it prohibits the extraction of non-concurrent information.

However, the Revised Notice did not go as far as the Registrar wished and the credit reference agencies will be allowed to extract information on other individuals who have lived as a member of the applicant's family. The exception to that is that they are not allowed to make such an extraction where the agency has information to show that there is no financial connection between the applicant and the third party. The decision of the Tribunal should take effect from 31st July 1993, so credit reference agencies and lenders will have a year in which to adjust to the revised rules.

Meanwhile, the Registrar is trying with all the parties concerned to reach a common understanding of the future requirements. The Registrar is also writing to all individuals who made complaints over the past few years regarding credit information giving them details of the Tribunal's decision.

New Data Protection Challenges

Police Data

Pan-European Law Enforcement: The police and other control authorities in the Member States of the European Community are moving towards greater co-operation and are taking steps to cope with the suppression of internal border controls that is about to become a reality over the next few years. These collaborative efforts are supported by information systems to facilitate the rapid exchange of information between the

appropriate authorities and the different countries concerned.

Three examples of such information systems are: the Schengen Information System, Customs Information System, and Europol. The common feature of all these systems is that the data is supplied by the relevant authorities, collected centrally and disseminated to the relevant authorities again for enforcement purposes. All of them will operate under Conventions (the Schengen Convention is one example, of which the UK is not a member.)

Within the Schengen Convention and other treaties there are specific data protection provisions, for example, the categories of data that can be held are defined, who may use the data, who may have access to it, and for what purposes, rules for retention and deletion of data, rules for independent supervisory authorities at the national level, and also rules as to a joint supervisory authority at the international level. The DPR will not be involved in the regulation of Schengen Convention but he is involved in customs co-operation and Europol.

The National Criminal Records Collection The Home Office carried out a scrutiny report on the national criminal records collection which was published in October 1991 - *The National Collection of Criminal Records, Report of an Efficiency Scrutiny.* The DPR contributed to that study. The report has made several recommendations concerning criminal records and its management. For example it advocates a single national computerised system; the establishment of clear ministerial accountability for the use of content of criminal records collection running through a self financing agency separate from the police; it advocates that there should be links to other criminal justice systems; and that there should be wider use of criminal records for vetting purposes, but within statutory guidelines which will be laid down by Parliament. The report recognises the data protection requirements, in particular the Registrar's suggestion for the development of more sophisticated weeding for criminal records. There will be further consultation on this study especially on the question of access to criminal records and its disclosure.

Police National Computer and HIV/AIDS The DPR has received complaints on the holding of information on HIV/AIDS status of individuals on the Police National Computer. The relevant information on HIV is held and maintained as a warning signal, one of several, to alert police officers of potential risks for themselves or others. Furthermore, there is no retrieval facility which could enable the police to retrieve all records of those people. The Registrar had to assess if it were relevant to the police to hold such information.

The Registrar studied a number of background papers including the Government's Advisory Committee on Dangerous Pathogens, which has a report on HIV infection in an occupational setting. He concluded that he could not say that it was in general, excessive and irrelevant for the police to hold such information as there is a small but foreseeable risk of police officers being infected by someone who is carrying HIV. Therefore, this was not considered a contravention of the Data Protection Act. However, he will still consider individual's complaints such as whether the holding of the information is consistent with the requirements of the Act.

National DNA Profile Plan The Registrar expressed his concerns about suggestions from the Home Affairs Committee of the House of Commons and the Metropolitan Police Commissioner that a national data bank of DNA profiles of the male population in the UK would be a good procedure. Contacts were made by the DPR's office with the Metropolitan Police Forensic Science Laboratory who held a database of around 3,500 profiles many of which are from people who had subsequently been eliminated from suspicion. The question raised here relates to the Sixth Principle of keeping data any longer then it is necessary, and there is also the conflict with the Police and Criminal Evidence Act 1984 which addresses the issue of the retention of fingerprints. usually destroyed in such circumstances. In that case, the Metropolitan Police deleted those files from

their databases voluntarily. The Metropolitan Police do, however, express the wish to retain DNA profiles for research purposes.

Regarding the possible establishment of a national data bank on DNA profiles, there have been many practical reasons why it is not feasible at present. Nevertheless, techniques are being developed, particularly digital DNA typing, which makes these a real possibility.

Confidentiality of Health Data

There has been a great pressure on the use of patient confidential information, required not only for provision of clinical care but also to support the demand of the internal market, due to the reforms in the National Health Service. The NHS management executive decided to produce a code on security of confidential information, which was welcomed by the DPR.

The Department of Health was against a code of confidentiality of personal health information but it explained that the common law duty of confidentiality applies to personal health information held for advice, treatment and health care of patients and for related management purposes within the NHS. However, the Registrar is not convinced that the common law provides as good a constraint on the use and disclosure of personal health information as could be provided by a statute.

The question of personal data also raises concerns within the NHS. The principle of *fair obtaining* applies to personal information obtained for health purposes as much as it does for marketing purposes. The requirements of notification are the same; and the requirements of opt out may apply. The use of personal information for research also gives cause for concern. The DPR is examining the circumstances in which a patient providing information for his or her health care should be given the opportunity not to have that information used for medical research.

Data Matching

This is the technique of comparing or merging two or more sets of records, particularly records established for public administration purposes. The DPR drew attention to data matching two years ago when he appeared before the Home Affairs Committee. It recommended that there should be clear proceedings governing the merging of files. The Registrar will draw up suggestions for a framework of regulations that might be introduced in the UK.

Calling Line Identification

CLI or Caller ID is a facility that allows a recipient of a phone call to see the caller's number displayed from the time the telephone first rings. The strongest reason advocated in favour of CLI is the deterrence to malicious calls making it easier for recipients to decide whether they want to answer the call.

There are some privacy concerns about this feature; it is prejudicial to the ex-directory system, and it allows cross reference to other data and its enhancement. The Registrar expressed his concerns about CLI and decided that the introduction of CLI is a matter within his jurisdiction because it involves the processing of personal data. Universal mandatory introduction of CLI display would lead to unfair processing of personal data by the network operator and should only be introduced with safeguards. The safeguards comprise mechanisms for blocking the display, and it should be available to all subscribers for whom CLI transmission is possible. Furthermore it should be simple to operate and free of charge. There are apparently no technical difficulties on introducing free blocking mechanisms on CLI even for subscribers on analogue exchanges.

This report is an edited version of a presentation at July's Privacy Laws & Business 5th Annual Conference, Cambridge given by Dr. John Woulds, Senior Assistant Registrar, Office of the DPR.

This report is by Deborah Fisch Nigri who is completing a doctoral thesis on computer crime in the commercial law department, Queen Mary and Westfield College, University of London.