THE UK DATA PROTECTION REGISTRAR ATTACKS ILLEGAL PERSONAL DATA MARKET

The UK's Data Protection Registrar, Eric Howe, has used his final annual report before retiring to spotlight and attack the UK's illegal black market in personal data. In some ways, the pattern of corruption is worse in the UK than previous examples we have covered in Spain and Australia. In the UK, the Data Protection Act has been fully in force since 1987, unlike Spain where the police could not find an appropriate statute under which to prosecute the alleged data traders (PL&B October 1992 p.3) or Australia where the law covers mainly the public sector (PL&B June 1993 pp.14-18).

A market in personal data

Mr Howe expressed his concern about the existence of a market in the UK, trading in confidential personal information. The allegations, initially made by *The Sunday Times* in late 1992, were confirmed by the complaints cases and investigations by the Registrar's Office. There seems to be an established market in which it is possible to obtain a wide range of confidential information about individuals. Some of this information appears to derive from sources such as bank accounts and tax records. Whilst there is no doubt as to the existence of such a market, its size is not known. Further inquiries are needed before any firm conclusions are reached.

How is information unlawfully obtained?

There are several sources:

- an employee within a data user's organisation making an unauthorised, illegal disclosure.
- an outsider who deceives a data user's employee in order to gain access to personal data.
- information service providers, such as credit reference agencies which widely disseminate sensitive data. This may be used for unlawful purposes.

What legal action can be taken?

The Data Protection Act can deal only partly with some of these problems. For example, it is an offence under the Act knowingly or recklessly to disclose personal data to any person not specified in a data user's register entry. However, there seems to be little legal remedy against a third person who obtains personal data from a data user's employee by deception. It may be possible to take action against such a third party on the grounds of aiding, abetting, counselling or procuring an offence under the Data Protection Act, even though the person who committed the principal offence had no intention of doing so.

An appropriate level of security

Data users are required to have appropriate security measures to protect the personal data they hold. This can play a particularly important part in preventing unauthorised access to personal data (see p.21). However, whilst the Computer Misuse Act 1990 may be of some relevance in this context and the above-mentioned prosecutions may prove possible in certain circumstances, neither of these provide an adequate answer to Registrar's concern about the activities of third parties.

The police and criminal justice system

There are a substantive number of issues of concern within the police and criminal justice system. To list but a few:

- the content and lifespan of criminal records
- putting old criminal records on computer
- automatic fingerprint recognition
- prosecution of police officers
- enforced access to criminal records
- HIV/AIDS markers on the police national computer
- codes of practice for police computer systems

- computer developments for the criminal justice system.

Among these issues, the Registrar has paid particular attention to the following:

The content and lifespan of criminal records

In view of the proposed future establishment of a single National Criminal Records System (NCRS), some data protection issues have been re-opened. One of these is the length of time for which criminal records should be retained and the criteria under which records would be deleted. The latest developments, such as the prevalence of certain types of serious offences, changes in sentencing policy and practice by the courts, and finally, the greater use of cautions by the police, made it necessary to review the agreed criteria for retention of police records.

Thus, in discussions with the representatives of the police, The Registrar has proposed the following modifications recognising the increasing concern in society about certain types of offence:

- Convictions involving indecency or violence, trafficking in drugs and possession of class A drugs are to be added to the list of those triggering retention beyond 20 years after the last conviction.
- Cautions would be retained initially for five years, with a commitment to analyse recidivism rates before the end of the five year period, thus enabling proper revision of this period.

Although acquittals, in general, will not be retained, there may be some exceptional circumstances which might need further consideration.

HIV/AIDS markers on the police national computer (PNC)

Convictions records held on the PNC allow for the inclusion of a warning signal whose purpose is to alert police officers to potential risks to themselves or others. One of the standard warnings is "may be hazard to others as a carrier of a contagious disease" and this can be supplemented by an indication of HIV/AIDS status. The Registrar expressed his concerns over this standard practice, questioning whether such an indication of an individual's *possible* HIV status was excessive or irrelevant for policing purposes and therefore in breach of the Fourth Data Protection Principle.

A recent guidance for the police service on HIV/AIDS, issued as a Home Office Circular, recommended that police forces should set up necessary training and education to establish standard hygiene procedures and should cease the practice of recording an individual's HIV status on police records.

In the light of these recommendations, the Registrar concluded that once these procedures are in place, the holding of HIV markers would be irrelevant.

Health data protection issues

In his report the Registrar has given his opinion on the following data protection issues in the National Health Service (NHS):

- the internal market
- administrative registers
- confidentiality of health information
- the need for statutory protection.

The development of "person-based" systems

The Management Executive of the NHS has recently launched a strategy to ensure that information and information technology are managed as significant resources for the benefit of individual patient care as well as for the population as a whole. The strategy is based on the following principles: development of "person-based" systems which hold individual health care records, greater integration between different NHS computer systems, and an extension of information sharing.

In view of these changes within the NHS, the Registrar will have discussions with representatives of the health care professions and other interested parties about the implementation of the strategy and its data protection implications.

NHS numbers as unique identifiers

In drawing attention to the data protection implications of reissuing NHS numbers, the Registrar welcomed the fact that the new NHS

numbers will not themselves incorporate personal information, such as date of birth. However, he is concerned that the NHS number could *de facto* become a personal identification number and be used so outside the NHS, without Ministers and Parliament having the opportunity to consider whether a national identification system should be established. Despite the Department of Health and the NHS Management Executive assurances that the new number will be securely held and used only for NHS purposes, the Registrar's concern still remains. He expressed fear that others will wish to use the new NHS number for their own purposes and that Crown Copyright may prove an expensive and cumbersome remedy to counter possible unauthorised uses of the number. Neither can the Crown Court Copyright prevent the use of the NHS number by other Crown Agencies.

Data protection and the media

The issues of data protection and the media and the way in which two human rights - privacy and freedom of expression - should be balanced has been much discussed. This discussion is becoming more urgent with the proposed EC Directive on Data Protection which allows Member States to exempt media from data protection legislation.

At present, there are no special exemptions for the media in the UK Data Protection Act 1984 and the Registrar's view is that any exemptions given to the media as a result of the EC Directive should only be such as are strictly necessary to reconcile privacy rights with freedom of expression. Mr Howe made it clear that, in his opinion, media should not be simply granted sweeping exemptions from legislation which protects individuals. "If, for example, subject access exemptions were specifically granted to investigative journalists, it would be difficult to understand why these would be wider than those available to the police."

The Registrar believes that modern newspaper systems bring much journalistic data within the cover of the Act. A newspaper publisher, as any data user, must register and comply with the eight Data Protection Principles. In, particular, he must hold accurate data and obtain information fairly and lawfully. Whilst the Act may not be the most appropriate way to deal with the wider issues of press regulation, it would have a role to play in specific cases. For, example, it might be considered that interception of a telephone conversation is a breach of the "fair and lawful" obtaining requirements of the UK Data Protection Act.

The code of banking practice

The Registrar also reported on various practices which were not in line with the Code of Banking Practice, which has been in force for over a year.

Firstly, some banks have made it a condition of trade that individuals give their express consent for passing their personal information to other organisations in the same group, which need not necessarily be involved in banking activities.

Secondly, the rules of confidentiality might seriously be undermined by the fact that many banks employ "host mailing," i.e. mailing selections of individuals on their own data bases with offers from other companies. Although the banks' customer information is not directly disclosed to other companies, they may ultimately come into possession of this information. For example, any response from a mailing directed to individuals with salaries above X, automatically means that these respondents have an income at that level.

It can be argued that a bank's duty of confidentiality can be breached not only by *disclosure* of customer information but by the *use* of such information. A solution would be to extend the requirement for customer consent, presently envisaged in the Code, to the users of a customer's information.

Big rise in complaints to the Registrar

The figures show that complaints from individuals to the Registrar rose from 1,747 in the previous year to 4,590 in the year ending May 1993. The main increase took place towards the end of the year following a TV

advertising campaign conducted on behalf of the Registrar's office in Scotland, the Midlands and the North of England, as well as on satellite TV. During the four weeks of the campaign, complaints were being received at a rate close to 29,000 a year. The campaign portrayed four examples of the kind of complaint which is commonly received and investigated by the Registrar's office. They related to credit reference, vehicle licensing records, criminal records and financial records.

Credit referencing complaints come highest on the list this year, and amount to some 63% of the total number of complaints. Following the pattern for the past few years, complaints about unsolicited mail have continued to fall.

Amongst the many other issues covered in the Registrar's report are:

- developments in local government,
- the finance sector,
- direct marketing,
- telecommunications,
- data security and
- data matching.

Ninth Report of the Data Protection Registrar HMSO HC 736. Price £13.25p

This report was written by Bojana Bellamy, a Privacy Laws & Business researcher

HIGHER COURTS INTERPRET CONTROL AND USE OF DATA

Prosecutions undertaken by the Registrar have virtually doubled. But the most significant innovation in the past year is UK Data Protection Act cases heard before the higher courts.

Data Protection Registrar v. Francis Joseph Griffin, Queens Bench Division

On Monday 22 February 1993, the High Court of Justice, heard an appeal by the Registrar against a decision taken by the Kingston-upon-Thames Magistrates on 1 June 1992. The Magistrates' Court had found the defendant not guilty of holding personal data contrary to Section 5(1) of the Act.

Mr Griffin, the defendant, was a self-employed accountant whose business was the preparation of accounts for clients. He owned his own computer and worked from home. He prepared and dealt with the accounts of clients. His method of working was to receive clients' accounting information in written form through the medium of invoices and other paper records. He would then use this information in a spreadsheet computer programme from which he would derive company accounts or private accounts for submission to the Inland Revenue and Customs and Excise for the purpose of VAT, Corporation Tax and Income Tax. He had never been registered under the Data Protection Act. When he was interviewed and asked whether he controlled the content and use of the data, he said that he did.

The case turned on whether Mr Griffin did actually control the content and use of the data on his computer or whether his clients did so. If Mr Griffin did not control the data, he would not be a data user and would not have to register; if he did control them, then he was liable to register.

Mr Griffin argued that he could not be said to exercise control as he had no right to use the data in any other way than to produce his clients' accounts. Although he manipulated the data to produce the accounts, that did not amount to control.

The Registrar contended that, although there were restrictions on the use of the data in terms of contractual and professional limitations, Mr Griffin still controlled the data within the meaning of the Act. He had a power to manipulate the data and as that manipulation involved the application of his professional skill, judgement and discretion, it went beyond merely acting on instructions given to him and he should be said to control the data.

The Court dealt with the specific question as to whether an accountant who receives "raw" information from his clients, which he puts on