HOW THE POLICE BALANCE THE CONFLICTING DEMANDS OF UK DATA PROTECTION ACT

Some of the most sensitive personal data is held by the police. A very careful balance has to be maintained between citizens' liberties and the state's obligation to preserve law and order. John Burrow CBE, Chairman of the UK's Association of Chief Police Officers Data Protection Group, reviews the impact of data protection law on the police and how they have responded.

Enforced access by job applicants to be a criminal offence?

Employers forcing job applicants to seek access to criminal records on themselves is becoming increasingly common, absorbing considerable police time and resources (see box p. 26). There is evidence that job applicants are being coerced into requesting their police records for quite inappropriate purposes such as obtaining work as a waitress or getting an insurance claim accepted by a loss adjuster! In the UK, the Data Protection Registrar has called for enforced access to be made a criminal offence, but there is some pessimism about whether doing so would be effective in curbing this practice.

Police need public confidence

In the Younger Report of 1972, the Home Office argued that police records should be outside the scope of privacy laws. But in 1978, the Lindop Report showed its concern about the heightened level of public anxiety if police records were to be kept secret. Indeed, when the police sought to develop further their use of computers, it concluded that there could be a backlash from the public on such proposals and the idea was abandoned. It was decided that for the police to be able to realise the full potential of their computers they had to retain public confidence.

Police computers a potential social control system?

In 1991, Liberty, the civil liberties group, issued a statement which voiced its concern about the proliferation of police computer systems. It said that it was widely recognised that the extent and the nature of information held by the police could provide one of the greatest direct threats to individuals' civil liberties, insofar as it potentially arms the police with social control system where every individual may be checked out.

This concern by Liberty was not unfounded. Police computers and databases could provide such a threat; and the police themselves have come increasingly to recognise that such systems have the potential to allow them to exercise social control.

It was against this background that the police looked at the Data Protection Act. There were three distinct phases following the introduction of the Act. The first phase was the fact that no one fully appreciated that it might affect their day-to-day policing practices. This led to a period of disbelief characterised by comments such as "You must be joking, this could not possibly apply to the police." Fortunately, this was closely followed by the third phase when the police recognised the importance of strict adherence to the data protection principles in order to retain public confidence. By doing this, the police could extend the use of their computer systems and gain public support at the same time.

Police need DPA controls

Indeed, the Registrar's Ninth Annual Report, published in 1993, said that the level of public satisfaction in the police use of computers was over 70%. The police seek to develop this degree of satisfaction further. It is not their intention to be exempted from the provisions of the Act.

Controls will have to be exercised even more stringently in an era where information is increasingly being exchanged between police forces in different countries, for example, via Europol and the European Drugs Unit.

The police sought to develop their adherence to the Act by a number of means. An Association of Chief Police Officers' Code of Practice was published in 1987. This code was supported by the Registrar on the grounds of the positive effect it would have in individual forces, and indeed, on individual officers, in recognising and paying attention to the principles of the Act. Similarly, a training program was introduced followed by a poster campaign to increase awareness. Now the majority of police personnel recognise the importance of the Act. There have been a very limited number of occasions when a police officer has accessed information in a computer system and disclosed it; and there have been a few other breaches of the data protection principles. These cases ended either in the criminal courts or in police disciplinary action. Such cases have been given prominent publicity within the police service, which has helped to reinforce the message that the data protection principles do affect them.

Unauthorised disclosures lead to better data security

One of the principles of particular concern is security; mainly disclosure of information by the police which has caused some concern within the community. This issue has been tackled in a number of ways. In addition to physical security, such as locks on doors and physical checks on personnel, there has been an increase in logical checks of the computer systems, such as logging transactions.

A few months ago, a BBC *Panorama* program alleged that there has been an unlawful disclosure of information on the Police National Computer (PNC). However, the police was able to check the logging of all transactions during that period and found no indication of a breach of the principles. Consequently, the police are still seeking a retraction from the BBC.

Audits introduced for national police computer systems

The extension of the scope of two police database systems, PHOENIX (the enhancement of the Police National Computer) and the National Fingerprint Identification System (NAFIS), has aroused some concern about the retention of criminal records and the national computer database on which they will be held. Detailed discussions have already been held with the Registrar as to how long criminal records should be kept on PHOENIX. (One European country keeps criminal records even after the person has died which is, indeed, excessive).

An agreement was reached with the Registrar on the majority of the issues concerning the retention of criminal records. The police have also undertaken to carry out a review of the retention periods. This will be possible as the computer system which is being adopted has the facility to conduct audit checks over a period of time. This could provide valuable information on the optimum duration for retention of different data. For instance, currently the police retain *cautioning of persons* data for three (shortly to be extended to five) years, as it may need to be cited in court. An analysis of usage should show whether five years is excessive or otherwise. Thus, the importance of using the computer system to analyse its data in order to devise a more accurate policy is something which is to be welcomed.

The implication of using PHOENIX, a national system, means that a common approach to maintaining criminal records can be adopted, as regional forces will no longer need to retain a separate local record system.

The other benefit associated with the PNC is the National Fingerprint System. This is a major development which will hold records of all fingerprints held by the police. The NAFIS will enable searches to be conducted across the 6 million records held on the national database.

Delays to the development of the National System by the Home Office prompted one regional force, Hampshire, to go it alone and develop a local system. This initiative has been successful to the point that some 38 other forces have joined a managed consortium to develop the system further. However, the National System will have a wider scope. It

will have a identification system whereby, for instance, a person arrested one evening may be identified by fingerprint records on the database and the courts will have up-to-date information by the following morning.

New Police National Network

In addition to the National System there are the so-called *in-force* systems. The national computer has had its own network linking these systems for several years, yet the relationship between the in-force systems has been somewhat limited because of incompatibility between them. This issue is now being addressed with inter-operability as an essential element. The most significant change relates to the introduction of a Police National Network (PNN) whereby all transactions between the national computer and police forces, and between the police forces themselves, will go through the PNN. This facility will become available over the next 9 to 12 months. A major concern is security over that network. In view of this, the Home Office contracted a private consultancy to investigate and advise on the whole issue of security. A comprehensive and detailed report was produced on the security of the PNC system and the recommendations of the report will be analysed and implemented, where appropriate, over the next few months.

Police to extend use of sensitive data?

Police forces across the land are being urged to extend their use of sensitive data:

- to *disclose* information more often than they do at present (see box); and
- to *hold* more information more than they do at present.

The police are firm in the view that it is essential that they retain public confidence in their use of computers. They want the public to be aware of both these issues, and to be fully involved in them through public debate; and the government to take decisions on them. It is even possible that the Data Protection Registrar will be involved in those discussions.

Pressure to retain more information

There is also pressure on the police to hold and retain *more* sensitive information, despite the fact that they are already under attack from

PRESSURE FOR POLICE TO RESPOND TO EMPLOYEE VETTING REQUESTS

The pressure for greater disclosure comes from the increased demands from employing organisations for vetting. At first, they were about persons who have access to children and, indeed, one can see the case for giving education authorities information regarding prospective employees. Then, taxi drivers became subject to enquiries as many authorities use taxi services to transport children to special schools, for instance, and they considered that the drivers should be vetted before being given a licence. A policy has now been agreed for the police to pass this information to the education authorities.

The problem arises that as soon as the police agree that one group of people should be vetted and authorise the information to be released, another group steps in and requests the same facilities. Thus, the position of those that care for the elderly is now under scrutiny. There is also a requirement for applicants to security firms to be vetted, especially those engaged in the special security areas of banking.

As a result, there is a great deal of pressure on the police to vet more people, and this situation leads to a perceived reluctance by the police to accede to these requests. One problem area, related to the Data Protection Act, is the question of the enforced data subject access request. If the police will not disclose the criminal convictions then the potential employer will require the applicant to make a subject access request. Some employers go as far as giving them a self addressed envelope and a £10 search fee. Naturally, if the person is anxious to get the job, he or she will comply with this requirement. The police have evidence that this practice has been going on, and that the amount of this type of subject access has increased dramatically - twice as many this year than in the previous year. This is a matter of considerable concern.

libertarian groups for holding too much information. Yet there are cases, notably the child molester Frank Beck, who was employed as a manager in a local authority children's home. It was widely said that the police should have retained the information on those incidents where allegations against him had been made. Had a record been maintained of allegations over a period of time, as he moved from one police area to another, it would have become obvious that he was highly suspect and should not have been employed in that job. However, the police do not hold that sort of information.

National Health Service (NHS) Trust legislation also creates problems in this area. Under the *Care in the Community* provisions NHS Trusts are now required to keep a supervision register of all mentally ill persons in their jurisdiction. These records contain information about the person's background which will include any relevant criminal convictions. Holding such information may be valid if the person, or the community, is at risk. However, the NHS goes even further in asking the police to inform them of any other incident in which the person was involved that might affect his treatment. The police think that these requests are too broad.

Children at risk is another area of concern. This is a register held by the local Department of Social Services of children that are considered to be particularly vulnerable to damage due to their personal circumstances. It is argued by some that as police are regularly sent to investigate domestic incidents they should have such information regarding the family or the child. To enable this policy to work, the Social Services would need to inform the police of what are sometimes just unproven suspicions.

Closed circuit television needs controls

Scepticism has also been voiced about the effectiveness of closed circuit television in public places - could the large investment in this equipment not be better spent on an increased police presence on the streets? Does it have an impact on anti-social behaviour as well as crime? Should these systems be subject to regulation or statutory control?

The police are anxious that the use of closed circuit television (CCTV) should be controlled by regulation; in the first instance by voluntary means, or by statute, if necessary. They think that the use of CCTV in public places is indeed an invasion of privacy and needs to be controlled. The benefits have been well proven in crime prevention and the reduction in social disorder. However, it must be recognised that it can be used in a variety of ways and it is interesting to see the question of closed circuit television coverage in terms of data protection. Indeed, the principles of the Data Protection Act apply to CCTV. Within the principle of fair obtaining there is provision for putting stops on cameras to ensure that they cannot film private homes or areas.

Police work within data protection law

The police do not want to be secretive or stay outside data protection and privacy laws, but rather that they want to be an integral part of them. There are, of course, the exemptions which apply to the police, such as prevention of crime and apprehension of offenders and the EU Directive recognises this as an essential requirement in certain defined areas. However, the exemptions should be limited to matters such as national security and crime prevention.

This report was prepared by Dr. Deborah Fisch Nigri, a *Privacy Laws & Business* consultant. It is based on a presentation given by Mr. John Burrow CBE, Chairman of the UK's Association of Chief Police Officers' Data Protection Group, to the *Privacy Laws & Business 7th Annual Conference* in July this year. For further information, contact John Black, Data Protection Officer, Essex Police. Telephone: 0245-452663. Fax: 0245-452127