PRIVACY AND DATA PROTECTION

Background

A Data Protection Act 1984 now exists in the UK. It concluded some 15 years of debate and discussion on the subject of privacy and computers, terminating in 18 months of Parliamentary activity.

I propose to use the UK Act and the arguments that have surrounded its contents to illustrate the change being brought about by the impact of micro-electronics, by other technological developments, many of which are becoming related to each other, and by the continuing flow of ideas in the pure sciences which are reflected in technology. A change is taking place in the concepts and principles upon which national, international and global economic, social and political activities are based. The UK Act is a symptom of this, in some respects a reluctant symptom.

The Act, and the Council of Europe Convention upon which it is based, indicate growing acceptance of a movement towards a more open system of both government and commercial use of data and information; It is probably correct to say that most, if not all, organisations of mankind revolve around the recording, processing and dissemination of data and information. From notches in sticks of wood, incisions in clay tablets, writing on scrolls to printing, radio, telex, television, and now to current forms of data handling and telecommunications. Historically the ability to form and understand written marks as distinct from speech has almost a religious significance. Inevitably

those individuals possessing such knowledge were often reluctant to see their position of eminence eroded in any way. However, the spread of literacy and the appearance of large scale production of books and paper, in relative terms, allowed a more organised and informed pattern of commercial and political activity to emerge based upon a more informed populace. New laws, copyright being one example, new structures, new attitudes all developed over a period of time, although the spread of literacy and information did cause some social unrest. Science cannot and should not develop in an atmosphere unrelated to social change and social restructuring. Computing science is typified by extremely rapid developments in both technology and techniques, in a time scale which does not appear to have an historical precedent.

In the late sixties the subject of privacy became a matter of public debate in the UK. It was initially shown by the appearance of two private members bills in Parliament, not supported by the government. However, pressures did result in a Parliamentary Committee being formed which reported in June 1972.

The British Computer Society had formed a Privacy Committee in 1969 and submissions from this committee were made to the Parliamentary Committee in 1971. Contact was also established with similar activities in other countries. It was interesting to discover the differing national attitudes towards personal data and its use, and the surprise felt by the citizens of these countries towards other national attitudes. In the UK it has been said that the populace tend to trust government and mistrust big business, an opposite public view to that in the United States.

The UK government tends to make all its data and records not available to the public, in Sweden the opposite view prevails.

The British public regard any suggestion of personal documentation or identification cards as an intrusion on civil liberties, in other countries they take them for granted and each is puzzled by the other's attitude.

In the UK this resulted in a reluctance on the part of successive governments of differing political creeds to take any action on the privacy question, a reluctance also shared initially by the Civil Service. This has resulted in the UK being behind many other countries in the time it has taken to formulate legislation.

Debate in Parliament also reflected many contrary and dissenting opinions on the proposed legislation, once this proposed legislation finally appeared in December 1982. This is now history. In order to ensure that comments on the implications of the UK Act are appreciated it is desirable to have an understanding of its details. The Data Protection Act of the UK is a complex document, as statutes usually are. It reflects much of the content of the statutes in other European countries, all of them being designed to meet the requirements of a Council of Europe Convention. The UK Act does the minimum necessary to meet this Convention, some statutes in other countries go further.

THE DATA PROTECTION ACT 1984

1. Introduction

- The Data Protection Act was enacted on the 12th of July 1984, it starts to come into effect on the 12th of September 1984.
- It will affect most organisations using computers of any type, mainframe to microcomputers. One objective of the Act is to allow the UK to ratify the Convention of the Council of Europe for the Protection of Individuals with regard to the Automatic Processing of Personal Data. The UK is a signatory to this Convention and its requirements become mandatory on all signatories once five members have ratified. The Convention reflects an international trend towards regulating the use of data in a technological environment.

- The Act has some direct security requirements and some legal obligations which can equally result in security situations. It is proposed to give an outline of the contents of the Act and to then comment on the specific security implications. An understanding of the Act is necessary for the security needs to be appreciated.

- The Act establishes a Data Protection Registrar who will maintain a register of personal data users and computer bureaux and have powers to ensure that personal data are used in accordance with the Data Protection Principles which form part of the Act.

- Data subjects are given certain legal rights

including that of access to data recorded about them, and in certain circumstances, to compensation. A tribunal is set up to whom a data user may appeal against decisions of the Registrar.

2. Definitions

- Definitions are given to expressions used in the Act, sometimes tortuously legal in the words used.

- "Data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose. In other words processed by a computing facility by means of a computer program. This excludes manual systems as such, although they are included in some other countries.

- "Personal data" means data consisting of information which relates to a living individual who can be identified from that information. The conditions of the Act cannot be circumvented by coding or disguising to whom the personal data refers.

- "Data subject" means an individual who is the subject of personal data. The subject can be referred to directly or indirectly and may form one of a group. The position of partnerships and individuals or groups trading under trading names should be considered, they are also data subjects. The distinction is between "natural persons" or people and "legal persons" or companies.

- "Disclosing" in relation to data includes disclosing information extracted from the data. This definition would embrace an answer to a telephone inquiry where the information is provided via a visual display to an employee answering the telephone.

- "Data user" means a person who holds data and a person holds data if:-
  - The data forms part of a collection of data processed or intended to be processed;
  - That person, alone or jointly or in common with others, controls the content or use of the data comprised in the collection.

- "Computer bureaux" are defined as activities in which a person provides other persons with services in respect of data and you provide such services if:-
  - As agent for other persons you cause information held by them to be recorded or processed or
  - You allow other persons the use of equipment in your possession for recording or processing information.

  This does not involve a company who leases out equipment, they are not a computer bureau or a data user. Some organisations will be both a data user and a bureau.

- "Processing" is defined as amending, augmenting, deleting or re-arranging the data or extracting that information constituting the data and performing any of these operations by reference to a particular data subject.

- "Scope of Definitions", do not attempt to attach your own meaning or some industry definition to the words in the Act. The words in the Act mean what the Act says they mean and the definitions have been defined in legally understood terms so as not to leave any loop-hole.

- "Exclusions" - Basic word processing as such is excluded and the definition of processing in the Act specifically covers this point. But it is only elementary text preparation and not any selective form of processing.

  The term "by reference to a particular data subject" in the definition of processing would exclude any record in which names may appear but no computer program exists which may process the data to select, choose or identify by name, personal category or a selective category.

3. The Data Protection Principles

Background

. These principles are contained in a schedule to the Act. In legal understanding they do not have a direct meaning, they are present to guide both the data user and the registrar as to how data should be handled. They come from principles given in the Convention of the Council of Europe (C of E) which originated from principles expounded by the British Computer Society (BCS) in 1972.

. The eight principles relate to the manner in which personal data are obtained and processed; the purposes for which data are held; the manner in which such data are used or disclosed; the quality of the data, including their accuracy and adequacy; the period for which data are retained; the right of the individual to seek confirmation that data are held about him, to see the data and to have such data corrected or erased where appropriate; and the taking of appropriate security measures to protect the data. The first seven of the principles are relevant only to data users; the eighth, in regard to security measures, is relevant to both data users and computer bureaux.

The Principles

. The principles and their meaning are:-

1. The information to be contained in personal data shall be obtained, and personal data should be processed,

fairly and lawfully

- Regard shall be paid to the purposes for which the data is held and the method in which it was obtained particularly if the person from whom the data was obtained was deceived or misled as to the purpose for which it is to be held. For example, failure to disclose fully the purposes to which the data is to be put and whether that purpose would involve disclosure of the data or information derived from the data to any third party.
- Information shall be treated as obtained fairly if obtained from a person who under an enactment or similar instrument imposing an international obligation is authorised to obtain it.
- It is interesting to consider the implications if data is processed by "pirated" software with or without the knowledge of the organisation owning the data and can this be considered as "fair".

2. Personal data shall be held for one or more specified and lawful purposes.
   - These must be the purposes registered. It will not be sufficient to specify the purpose directly to the data subject or to publicise the purpose.

3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with those purposes.
   - Those purposes will be those registered and any disclosures can only be made as defined and accepted in the registration.

4. Personal data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose.
   - This therefore excludes any speculative collection of data and a definite relationship must exist between each item of data held and the purpose for which it is held.

5. Personal data shall be accurate and, where necessary, kept up to date.
   - Although the Act defines inaccuracy as data being incorrect or misleading as to any matter of fact, care should be taken in recording opinions.
   - Data received from a third party should be indicated as such and if the subject of the data feels it to be misleading then that must also be indicated.

6. Personal data held for any purpose shall not be kept for longer than is necessary for that purpose.
   - Data may be kept indefinitely when it is for historical, statistical

or research purposes, this purpose would, of course form part of the registration.

7. An individual shall be entitled:-
   - To be informed by the data user whether data is held of which that individual is the subject.
   - To have access to such data.
   - Where appropriate to have such data corrected or erased.
   - A fee is permitted to be charged for providing access to the data.

8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.
   - Appropriate would need to be measured against such points as the nature of the data and the harm that would result from its misuse. Other specific points mentioned in the Act include regard to the place where data is stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data.

4. Registration and the Registrar

Registration

A Registrar will be appointed under the Act and will maintain a register of data users who hold personal data and of computer bureaux who provide services in respect of personal data.

A data user or a computer bureau will have to register their activity with the Registrar and the data user will need to describe the data held, the purposes for which it is held, the sources of the data and the persons to whom it is intended to disclose the data. Where it is proposed to transfer data outside the UK then those countries must be in the registration of the data user. One or more addresses must also be given for receiving and dealing with requests from the data subject for access to data.

A computer bureau will not, of course, know any details of the data for which it is providing services and its registration will be a simpler one.

The Registrar may refuse an application if the information is insufficient or it seems that the purpose may contravene the data protection principles.

Inevitably a fee is involved in registering, but a registration may last for three years before renewal is required. Registration can give immediate rights to hold and process data and may be an automatic process, unless the data user has been refused registration in the past two years or has had other problems with the Registrar.

The powers of the Registrar relate to data users who have applied for registration or who are registered.

For this reason to hold and process personal data without being registered, and therefore being outside the orbit of the Registrar, is a criminal offence to which no defence is permissible under the Act.

The Registrar

For data users who have registered, and the Registrar may refuse registration, the Registrar has powers to enforce and insist that the data user complies with the data protection principles.

These notices give the basis of the powers of the Registrar:-

- An enforcement notice; you will do this in this period of time.
- A de-registration notice; this removes all or part of a data user's registration, it may follow an enforcement notice which has been ignored. This will mean that to continue to hold or process the data concerned will involve a criminal offence with no acceptable defence.
- A transfer prohibition notice; you will not send this data to that country. Different conditions exist for countries who are not bound by the Convention of the Council of Europe and those who are.

The Registrar is meant to hold a balance between the data user and the data subject, provided the data user has registered.

5. Appeals and the Tribunal

The data user, but not the data subject, may appeal to a Tribunal against any decision of the Registrar. This Tribunal operates under the Council for Tribunals and will include people with a specialised knowledge of computing and representation on behalf of the data subject in addition to a strong legal content.

The Tribunal may overturn a decision of the Registrar, may confirm any decision or may substitute a more onerous decision than that proposed by the Registrar.

The decision of the Tribunal is final, appeals from its decisions can only be made on points of law.

6. Powers and Penalties

A warrant may be issued by a circuit judge authorising the Registrar or his staff to enter, search, inspect and seize documents or material if reasonable grounds are shown that an offence has been committed or a contravention of the data protection principles has occurred.

Offences may be criminal as well as civil. Where the offence has been committed by a body corporate an officer, director or manager of that company, or any person purporting to act in such a capacity, can also be held guilty if their actions or neglect contributed to the offence.

7. Rights of Data Subject

The Register

- The Data Protection Register will be available for public viewing and, for payment of a fee, a certified copy of a registered entry can be obtained.

- A key element of the Data Protection Act is the right for data subjects to obtain access to personal data stored about them. This is stated in the seventh data protection principle and is a matter in which the Registrar is entitled to intervene. The access right itself is ultimately enforceable through the civil courts. An individual is also entitled to know that no data is stored about him or her.

Subject Access

- Data subjects will have the right to be informed by any data user whether the data held includes personal data of which that individual is the data subject. A copy of that data must be supplied on request, in an intelligible form. Some restrictions may be applied by the data user to the data supplied to the subject if the data in some way relates to another person. A fee may be requested subject to a statutory maximum. Each entry in the register is a separate entry, requiring a separate request and a separate fee. A period of 40 days is allowed for data requested to be supplied and it may need to be as it existed at the time at which the request was made. It would be an offence for the data user to make any changes which were not part of normal routine processing and up-dating.

Multi-registration

. Individual data users will have to decide on the advantages or disadvantages to them of a number of separate registrations against a multipurpose or all-embracing registration. It may be a situation in which a single request for access for a single fee could create a considerable amount of effort at a high cost in satisfying the request.

Complaints

. A data subject may, of course, complain to the Registrar, who may or may not decide to take action. The Registrar has a statutory duty to promote the observance of the data protection principles by data users and computer bureaux.

Damages

. A data subject who suffers damage by reason of the loss, destruction, unauthorised disclosure or inaccuracy of personal data shall be entitled to compensation and may also be entitled to have the data rectified or erased. It is probable that distress may be taken into account in assessing any compensation awarded to a data subject. This action would need to be taken through a court, the Registrar cannot award damages; the civil action may well, however, follow some action by the Registrar.

8. Exemptions

. Exemptions exist from all or part of the Act. They are fewer in scope than comment or criticism would lead one to believe.

National Security

. Total exemption is given for national security data. This requires the agreement of a member of the cabinet, the Attorney General or the Lord Advocate. This could apply to data held outside government organisations if the relevant cabinet minister so decided.

Domestic

. Total exemption exists for personal data concerned with family or household affairs. Your home micro should not, however, be used for any form of business record without consideration being given to the Act possibly being applicable.

Limited use

. Total exemption is given for matters associated with an unincorporated members club or simple name and address lists used only for the distribution of articles to data subject. Be careful in interpreting this. A golf club or tennis club may be exempt if unincorporated, is only keeping records of members, and the data subject has agreed to the proposed use and disclosure of the data being held.

The example given by the Home Office on the simple use of name and address lists

is that of the delivery of copies of a church magazine.

Basic Payroll and Accounts

. Total exemption is also given for data held only for the calculating of remuneration of pensions or for keeping account of money paid or received for goods or services. This data may not be used or disclosed for any other purpose. This exemption only applies if the data are held exclusively for these purposes.

The data subject may give specific consent to disclosure in circumstances such as monthly payments to a trade union or medical insurance fund.

However, this exemption is, in practice, very limited and it may be more prudent for a data user to register. Not to register when holding personal data and where an action has occurred outside the scope of any exemptions, possibly innocently by a staff member, can create problems for a data user.

From subject access

. Exemption from subject access, but not from registration, is given for data held:-

- . for the prevention or detection of crime
- . for the apprehension and prosecution of offenders
- . for the assessment or collection of taxes.

This exemption does not restrict itself to data held by government organisations, the police as such are not mentioned. A data user holding data which is stated to be under one of these categories will need to state the purpose on registration and may need to satisfy the Registrar on the question of exemption from subject access. A data subject has the right to both complain to the Registrar and to a court if access is refused and the data user will need to justify the action.

Archival etc.

. Other exemptions exist for data held only for historical, statistical or research purposes. The Secretary of State also has the power by order, subject therefore to Parliamentary approval, to provide other exemptions from subject access.

Non-disclosure

. A data user may disclose data if satisfied that the request is made on the basis of the three exemptions given for subject access. In practical terms this is the current situation where, say, a request from a police force for data held by a data user may be acceeded to at the discretion of the data user if reasonable ground exist for believing it to be for matters connected with crime. It is not necessary for this purpose to be registered although the data user may be called upon to justify the action.

A court order to disclose data would be

obeyed regardless of the registered purposes. In addition data may be disclosed if it is felt that injury or damage to the health of any person may result if the data is not disclosed, an extreme example being a civil emergency.

9. Data held outside the United Kingdom

. Fundamentally this part of the Act is to prevent evasion of its conditions by processing in other countries. The Act cannot apply to data which both originates abroad and is processed abroad.

. Specific provisions are made in the Act for data originating in the UK and processed abroad or vice versa. This situation could apply to both data users and computer bureaux, and questions of data held being processed in different countries at different times may need study.

. The Act applies to data users who control the contents and use of data from within this country, and to persons carrying on computer bureaux who cause data to be processed or allow the use of equipment for processing from within the UK. As these persons are within the UK they are within the jurisdiction of the Registrar.

. The question of a servant or agent in the UK of a foreign organisation is dealt with by regarding that person as holding data on his own account. The provisions of the Act cannot be evaded by pointing to ultimate control abroad.

10. Timescales

Administration

. The Secretary of State following enactment of the Data Protection Act will give an "appointed day". Data users will be required to register during a six month period following the appointed day. For the following 18 months the powers of the Registrar are subject to some restrictions and any orders issued by the Registrar cannot have a compliance date before the end of that 18 month period. It will, however, be an offence for a data user or a computer bureaux to operate unregistered during that period. The 18 month period is to allow a data user time to effect any necessary changes required by the Registrar following the six month registration period. Basically the Act is in full force after the six month period.

Compensation rights

. The rights of the data subject to compensation do not apply before certain dates.

A subject has a right to compensation where damage is suffered as a result of the loss, destruction or unauthorised disclosure of data which occurs from a date two months after the date of enactment. This follows a convention that where legislation imposes new obligations there should be a short period of grace to allow those concerned to be aware of the provisions. In practical terms this means that a data

user is at risk of an action for damages for an event which occurs before registration. The effective timescale of the Act in some very pertinent aspects is far shorter than is generally realised.

- A right of compensation for damages due to inaccurate data can only apply to events which occur after the end of the initial six month registration period.

- A late amendment to the Act extends the right of compensation for the data subject to data which existed before the Act appeared. Compensation for inaccuracy, loss, destruction or unauthorised disclosure of data can relate to data which came into existence many years ago and was subsequently transferred into a computing environment.

11. The Security Implications

. From an understanding of the requirements of the Act it is apparent that organisations are at risk by failing to comply with the statutory details of the Act. This could be either by not registering when the Act requires it, or in having registered, to fail to comply with the registered details. Commercial and industrial advantage can be obtained by a rival manoeuvering a situation to ensure than an organisation infringes some principle or detail required by the Act. A situation of this type could be created inside the law and make it impossible, or at least unacceptable publicly, for an organisation to continue its use of computing facilities without change.

The security point is one of making the organisation secure in its continued and acceptable use of computing facilities.

. The eight data protection principles whilst equally valid do not necessarily carry equal weight in their effect upon organisations. The eighth principle which applies to both data users and computer bureaux is a specific requirement for "appropriate security measures". Naturally these are not defined although some illustrations are given in a schedule to the Act. The nature of the personal data is a point to which regard must be given but it must be accepted that a basic premise has been

frequently expounded that no data is harmless, and it may be necessary to produce evidence that the data is of itself harmless. Of course it may be harmful if correlated with other data.

- The Act makes a specific point of data storage, of measures programmed into the relevant equipment and to the reliability of staff. Storage is largely a physical question of access control, plus logging and recording of access. Programmed measures would be planned to deal with direct access control to the data. Reliability of staff is indefinable as a statistical criterion. All of these points are direct questions of security, they will involve a monitoring process on the relevant procedures adopted within an organisation.

- Security is an attitude of mind, as has been frequently said. The technology of information systems brings a new dimension into the subject of security. It is a matter for the trained security mind and outlook.

- We now have security measures required by statute within a computing facility. It would be unwise of any organisation to seek to evade the requirements of the Act. Political opposition to the passage of the Act in Parliament was to a great extent

focussed on amendments put forward to extend the effect of the Act on a data user. The Council of Europe Convention was formulated in 1981 and may itself be subject to future amendments, none of which are likely to reduce the scope of the requirements of the Convention. In defining rules and considering practices for handling of data it should be accepted that public accountability will be increasingly expected and "appropriate security measures" looked for.

DISCUSSION

Professor Tanenbaum hypothesised a situation where a large company owns small mini or microcomputers with files containing usernames and passwords, and asked if such a situation would legally bind the company to register under the act. Mr. Kenny replied that such situations were not covered in the act, since such informaation does not amount to personal data about individuals.

Professor Cohen remarked that the situations would be different if a person's name could be inferred from such a file, or if it contained names and addresses. Mr. Kenny concurred, but said that the real problem was recognising when situations might be relevant to the act at all. Of all possible offences under the act, the most serious is not registering a use of personal data at all.

Mr. Cowlishaw asked whether the act permitted an employee to see information held by his employer, for example salary plans. Mr. Kenny said that it did. It also applies to home computers, if they are being used for business offers.

Dr. Ratcliffe described situations where information was held about individuals, but such information can only be used with data issued by a third party, for example medical records containing people's medical numbers, where the mapping from number to name is known only by the National Health Service. Mr. Kenny replied that there would always be situations not adequately covered by the act.

Professor van Rijsbergen asked about the rights individuals had to have faulty information about themselves corrected. Mr. Kenny's reply was that such rights were un-neccessary - any institutions should be glad to have faults in its records pointed out. Professor van Rijsbergen didn't take such an optimistic view.

Dr. Beth asked for a clarification of the meaning of personal information; German laws had strict rules to govern this. Mr. Kenny gave some examples: names and addresses for distribution lists were regarded as free information, but could not be transferred to a third party without consent.