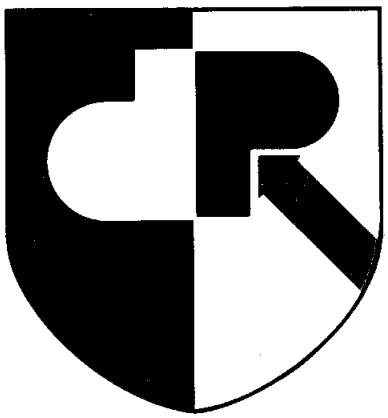
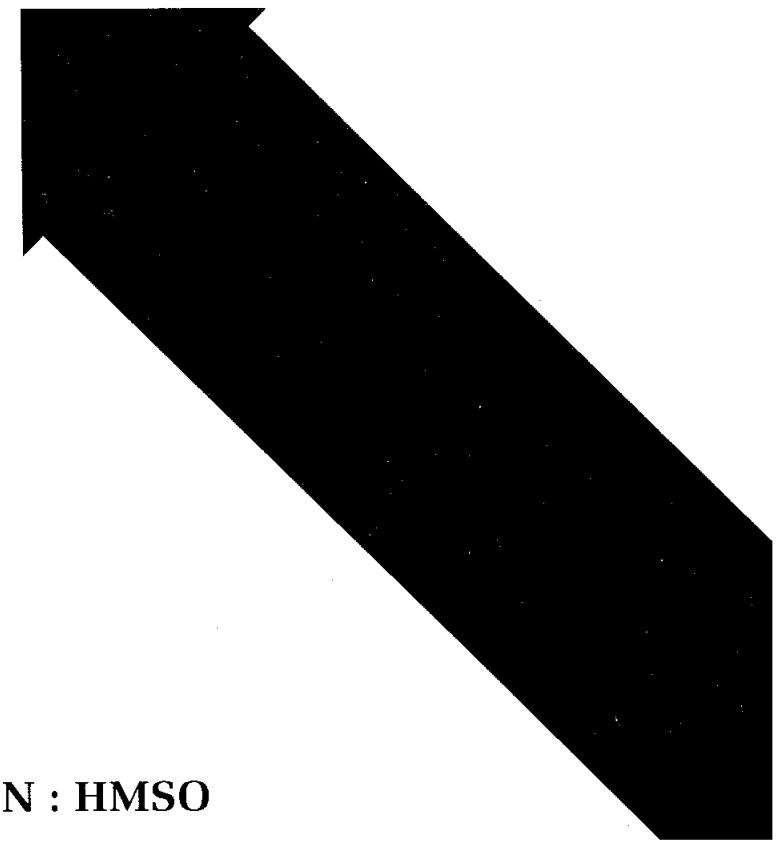
EIGHTH REPORT of the Data Protection Registrar June 1992



THE DATA PROTECTION REGISTRAR



LONDON : HMSO

EIGHTH REPORT

of the

Data Protection Registrar

June 1992

Presented to Parliament pursuant to Section 36(5) of the Data Protection Act 1984

Ordered by the House of Commons *to be printed*
14 July 1992

LONDON: HMSO

Contents

1 Introduction

This report is for the year ending 31 May 1992. In the public sector, new issues continued to arise both from new legislation and from developing uses of personal data. In the private sector, the year has seen the completion of the enforcement action against the main credit reference agencies in respect of their provision of third party information to lenders. Outside the United Kingdom itself, there has been an acceleration in activity with data protection implications at the level of the European Community.

I am pleased to record again my appreciation of the professionalism and enthusiasm of my staff. For about six months office conditions were very cramped following the end of the lease of premises outside the main office. The move to new offices, bringing everybody under one roof, has now been completed and I am grateful for the patience staff showed during these changes.

2 The European Community Dimension

The continuing harmonisation and integration of activities across the European Community (EC) will have an increasing effect on data protection in the United Kingdom. At present, this arises from the European Community's Draft Directive on Data Protection and from wider collaboration between member nations on law enforcement. This section sets out the current position on the draft directive and briefly reviews the collaborative activities.

(a) The European Community's Draft Directive on Data Protection

In my last annual report, I explained that the Commission of the European Communities (CEC) had, in July 1990, proposed to the Council of Ministers a package of measures relating to data protection. Of particular significance was a draft directive[1] which would substantially harmonise data protection laws in the Community.

Last year I set out my reactions to the draft directive. These are given in some detail in appendices to my Seventh Annual Report. I welcomed the added protection that would be given to individual privacy. However, I was concerned about the practicality of some of the proposals, such as the arrangements for the control of transborder data flows, registration by data users and the rather extensive application of data protection rules to manual records.

The draft directive has stimulated greater collaboration between the Data Commissioners of the EC nations. A formal grouping has been established which is meeting on a fairly frequent basis. At a meeting in the Hague in November 1991, the Commissioners adopted a common view of many parts of the draft directive. This view was forwarded to representatives of EC governments, to the Commission and to the appropriate committee of the European Parliament. It is pleasing to see that the Commissioners, each of whom has a different background of national legislation, were able to reach a good degree of agreement.

Discussions on the draft directive have continued within the Council of Ministers working party and in the European Parliament. The most significant development has been the formal opinion given by the Parliament on 11 March 1992. That opinion embodied many proposed amendments to the directive—some intended to strengthen the protection of individuals, some to relax the burden on commercial organisations. A number of these amendments are clearly responses to the intense lobbying by pressure groups which has taken place.

The draft directive must not create unnecessary bureaucratic burdens for data users. However, I am concerned that concessions demanded by sectoral lobbyists would reduce the level of protection given to individuals by the existing United Kingdom law. That would fly in the face of a declared aim of the draft directive—to

1. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data—COM(90)314 final—SYN 287.

ensure that there is no reduction in the existing level of protection given to individuals in EC member countries.

For example, those with interests in direct marketing have criticised the requirement to give people information about the intended use of data when it is collected from them. That criticism takes no account of the fact that the current United Kingdom Data Protection Act requires that information should be obtained fairly. I believe that the Act's requirement is, in practice, very similar to that in the draft directive. I return to this point in Section 3(d).

As to the future of the draft directive, I expect to see a thoroughly revised text from the CEC about the time this report is published. The Council of Ministers will then seek to reach a common position on this text. Following this there will be a further round of consultation with the European Parliament before final adoption of the directive. This suggests a finally approved directive by late 1993. Given a further two years allowance for the development and adoption of national legislation, it may be late in 1995 before we see a new United Kingdom Data Protection Act. I return to the draft directive in the Conclusions in Section 13.

(b) Collaborative Activities

Police and other control authorities in the EC Member States are moving rapidly towards greater cooperation as steps are taken towards the removal of internal border controls. Cooperative arrangements will be supported by computer systems which will facilitate the rapid exchange of information between the relevant authorities. The Schengen Information System, which is concerned with policing matters and immigration control, is the first example of this type of collaborative development. But discussions are also at an advanced stage between customs authorities and between drugs enforcement agencies.

Under each of these developments data will be supplied by relevant authorities in the participating States to a central system. From there, the data will be disseminated or made accessible to appropriate authorities in the other countries concerned. In some cases the central system serves merely to facilitate the exchange of information; in others, the central system includes an analysis function by which raw data from several different sources may be combined and enhanced to improve their intelligence value.

For each development, protocols need to be determined which will govern the cooperation between the different national authorities. These protocols are, or will be, formalised in international treaties. These treaties will provide the legal basis for establishing the support infrastructure, including the automated data processing. Data protection provisions are an essential and integral part of these protocols.

For example, the Schengen Information System will operate within the terms of the Schengen Convention which will bind collaborating States. As far as data protection is concerned, the policy is to rely on national regulations as far as possible. However, there are specific Convention provisions to reinforce national legislation where appropriate and to deal with possible conflicts between national approaches.

Thus, the Schengen Convention prescribes the categories of data and data subject which may be held and lays down constraints on who may have access to the data and the purposes for which the data may be used. The Convention obliges each participating State to have an independent national supervisory authority. It is expected that, in most cases, this role will be performed by Data Commissioners or their equivalents. It also establishes a Joint Supervisory Authority comprising representatives of each national authority. The role of the joint authority is to supervise, from a data protection point of view, the functioning

of the central system and to consider difficulties in the application and implementation of the provisions of the Convention.

The United Kingdom is not a party to the Schengen Convention and will not therefore be represented on the Joint Supervisory Authority. Nevertheless, it is important to keep fully informed of progress, not least because the Schengen Convention does establish a model for consideration for other collaborative developments. To this end I am pleased that a working party of the Data Protection Commissioners of EC States has been set up to discuss data protection issues in the context of cooperation in policing and related areas. This will allow those who are, and those who are not, parties to the Schengen Convention to learn from each other.

In contrast with Schengen, the United Kingdom is very much involved in the other two areas mentioned above. As regards the Customs Information System, I have been consulted by the Home Office and by HM Customs and Excise and have had the opportunity to comment on the draft protocol. In the case of the proposed Europol Drugs Unit, I am pleased to have been invited by the Home Office to participate in discussions at a very early stage and to take an active part in the drafting of the data protection provisions. One of my senior staff is involved in this work.

A particular form of collaboration concerns the arrangements for policing of the Channel Tunnel. This has involved my staff in immediate practical consideration of the data protection implications of international cooperation between control authorities. Discussions are continuing with the police and other relevant authorities and with the Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection authority. It seems likely that legislative measures will be taken, both in the United Kingdom and in France, to allow each data protection authority to supervise the use of personal data by its own national authorities in the Tunnel control zones, even though these extend onto the territory of the other country. Whilst this is an unusual arrangement, in that it effectively allows the law of one country to operate in another, it does seem to offer a practical solution to a control problem.

3 Some Issues in the United Kingdom

In this section I deal with a number of significant issues with which my Office has been concerned over the last year.

(a) Policing and Criminal Justice

The policing and criminal justice system is changing and developing rapidly. I have mentioned changes arising from greater European collaboration in Section 2, but, changes are not confined to Europe. This year has seen the launch of the National Criminal Intelligence Service (in April 1992). This body has taken over responsibility, amongst other things, for the former Units for National Drugs Intelligence and National Football Intelligence. The year has also seen the introduction of the new Police National Computer (PNC2). In parallel, the Home Office led Committee for the Co-ordination of Computerisation in the Criminal Justice System (CCCJS) has continued to promote greater integration and sharing of information between the bodies comprising the component parts of the criminal justice system.

This section reports some of the more detailed matters that have arisen during the year. The necessary contacts have been, or are being, established with a view to ensuring that data protection requirements are taken properly into account in each of the more important developments. The liaison with the data protection group established with the Association of Chief Police Officers (ACPO) is very helpful in this respect. Much remains to be done.

(i) *Warning Signals on the Police National Computer (PNC)*

An indication of an individual's HIV/AIDS status may be held in conviction records on the PNC. As a result of a complaint, I have considered whether this information is excessive and irrelevant and therefore a contravention of the Fourth Data Protection Principle.

Conviction records held on the PNC allow for the inclusion of a warning signal to alert police officers to potential difficulties, or of risk to themselves or others. One of the standard warning signals available indicates "may be a hazard to others as a carrier of a contagious disease" and this can be supplemented by an indication of HIV/AIDS status. The conviction records are held on persons charged with serious offences who have either been convicted or are awaiting trial for such an offence. No search facility is available which would allow all records containing a particular warning signal to be retrieved as a group and records are only retrievable individually. This position will need to be kept under review if more sophisticated searching facilities become available on the new Police National Computer System (PNC2).

The police state that information about a contagious disease is usually obtained from the individual concerned. Also, that the authority of an Assistant Chief Constable or above is required for the disclosure of HIV/AIDS markers outside the police service. It is not police policy to include a person's

HIV status as part of a disclosure of convictions records to employers or professional organisations.

Looking into the matter, I considered information from a variety of organisations and sources. Besides the police, these included Liberty, the Terence Higgins Trust and various background papers from organisations such as the Council of Europe. In particular, I took into account the views of the Government's Advisory Committee on Dangerous Pathogens, which has reported on HIV infection in an occupational setting. The Committee, whilst recognising that no cases of occupational infection had occurred outside the health care or medical research fields, believes that workers who have more occasional contact with bodily fluids in the course of their duties should take special precautions. Those mentioned by the Committee include emergency service workers, custodial staff and persons who may have to handle the dead.

Having considered the information available, it appears to me that there is a small, but foreseeable, risk of infection with HIV/AIDS which could arise in connection with policing activities. Accordingly, I am satisfied that, in general, the holding of a factual warning signal, including an indication of HIV/AIDS status in the PNC conviction records, is neither excessive nor irrelevant to policing purposes. However, it remains open for me to consider, in the circumstances of an individual complaint, whether the holding of such a signal is consistent with the requirements of the Act.

My staff will continue to consider the procedures used by the police service for verifying, deleting, disclosing and securing HIV/AIDS markers. The objective will be to ensure that sound procedures exist and are in full accord with the requirements of the Data Protection Principles.

(ii) *Criminal Records*

In my last Report I referred to the fact that the Home Office had established an Efficiency Scrutiny of the National Collection of Criminal Records. This was in response to concerns expressed by the Home Affairs Committee of the House of Commons. The report of the scrutiny[1] was subsequently published along with a Government foreword dated 22 October 1991.

The report makes a wide range of recommendations, among the most important being:

- putting all criminal records, from both national and local level, onto computer and integrating them into a single national system;
- adding cautions to the list of criminal records;
- establishing clear ministerial accountability for the use and content of these records;
- putting responsibility for running the system under a self-financing agency. This agency would take over ownership and day-to-day control of the records from the police;
- linking the criminal record system to other systems in the criminal justice sphere;
- allowing wider use of criminal records for vetting individuals in order to protect children and other vulnerable groups. Also to maintain

1. "The National Collection of Criminal Records"—Report of an Efficiency Scrutiny, Home Office, 1991 (£6.95).

standards of probity in jobs acknowledged by Parliament as subject to licensing or "fit and proper person" requirements;

— arranging for the vetting of individuals to be overseen and administered, within new statutory guidelines, by the record agency;

— balancing wider vetting by new safeguards to limit the risk of misidentification, to minimise the barriers to the employment of ex-offenders and to ensure that employers do not misuse criminal records information;

— limiting the range of exceptions to the Rehabilitation of Offenders Act.

The report is wide ranging and deals with a matter of considerable sensitivity. I was pleased to note the recognition of data protection requirements—in particular, acceptance of my suggestion for the development of more sophisticated weeding criteria for criminal records. On the other hand, I did not feel satisfied with the response to my concerns about "enforced subject access". I explain this problem in (iii) below.

Overall, I welcome the report. It should lead to a more open consideration of the control over the use and disclosure of criminal records. As the Government says in its response, the report's recommendations raise substantial issues of policy and practice. I look forward to the consultation paper on disclosures of criminal records which has been promised about the end of this year.

(iii) *Access to Criminal Records by Local Authorities and Employers*

I have, in the past, commented on the practice of requiring individuals to exercise their rights of subject access in order to reveal their criminal records to potential employers or licensing authorities ("enforced subject access"). It may well be proper to examine the criminal convictions of those applying either for certain classes of employment or for particular licences. However, this should not be achieved by a misuse of the rights given to the individuals under the Data Protection Act.

My concerns are well known to the Home Office, have been drawn to the attention of the Home Affairs Committee and were recognised in the recent Efficiency Scrutiny of the National Collection of Criminal Records referred to above. I have recommended that enforced subject access should be made a criminal offence. The Efficiency Scrutiny did not support this proposal, but further discussions with the Home Office have led me to believe that my view may become acceptable.

The practice of enforced subject access has been particularly prevalent amongst local authorities with responsibility for the licensing of hackney carriage and private hire vehicle drivers. Applicants for such licences are very often required to make a subject access request to the police and pass on details of their criminal convictions, unopened, to the licensing authority. In some cases details of criminal convictions have been published in documents to which the public have access under The Local Government (Access to Information) Act 1985.

The licensing authority is required to make a judgement on whether the applicant is a fit and proper person to hold a licence. These licensees carry vulnerable people and it does seem appropriate to me that checks be made, subject to proper safeguards on the use and disclosure of what may be very sensitive information.

The Road Traffic Act 1991 provides, with effect from 1 April 1992, that a licensing authority may send a copy of an application for a licence to the relevant Chief Officer of Police and request his views on it. The Home Office and Department of Transport have advised local authorities and the police on the subsequent procedures to be adopted for checking the criminal convictions of licence applicants. These procedures should obviate the need for enforced subject access and in general I welcome them. However, I remain concerned that the Home Office appears to expect only a gradual rather than immediate abandonment of the practice of enforced subject access by licensing authorities. I am pursuing my concerns with the Home Office and Department of Transport.

(iv) *DNA Profiles*

In my Seventh Anuual Report, I commented on suggestions which had come forward from the Home Affairs Committee and the Metropolitan Police Commissioner for large scale databases of DNA profiles. I remarked that establishing such databases calls for careful consideration of data protection requirements.

During the past year my staff have been actively pursuing this issue through discussions with some of the leading players in the field. It is clear that techniques are evolving at such a rate that, whereas until now talk of establishing large scale databases has been premature for a number of purely practical reasons, such a prospect may soon become a realistic possibility. The recent development of digital DNA typing is a major step in this direction. I will continue to keep this under review.

In parallel with the discussions referred to above, my staff have looked at DNA profile data held by the Metropolitan Police Forensic Science Laboratory. Data were being retained on people who had given samples in the course of criminal investigations and who had subsequently been eliminated from suspicion. This raises questions at least of compliance with the Fourth and Sixth Data Protection Principles, as well as being contrary to the procedures laid down in the Police and Criminal Evidence Act for the retention of fingerprints, which are destroyed in these circumstances. In the event, the Metropolitan Police decided to destroy the 3,500 such profiles held for investigative purposes.

The Metropolitan Police do however wish to retain DNA profiles for research purposes. If such profiles can be de-personalised and no longer linked back to individuals, this would allay any concerns. The issue remains to be resolved.

(b) The Health Service

Reforms in the National Health Service (NHS) have drawn a distinction between those who are responsible for assessing the health care needs of the population and for deciding on what priorities and standards are to apply in meeting them ("the purchasers"); and those who are responsible for providing that health care ("the providers"). Enhanced information systems are essential if the reformed NHS is to be both efficient and effective in its provision of services. Patient information is required not only for the provision of clinical care, but is increasingly in demand to support the new internal market and for management and planning purposes. The ways in which these increasing demands are addressed must be consistent with the requirements of the Data Protection Principles and must not compromise the confidentiality which the sensitivity of personal health data demands.

The development of the internal market has led to contracts for the provision of health care between purchasers and providers and an associated flow of patient information in what are termed "contract minimum data sets". I expect to publish a report on the content and use of these data sets during the summer. I am grateful for the helpful contributions made by many parts of the Health Service to this report which will outline the requirements of the Data Protection Principles. Other matters under consideration but not dealt with here include the prospect of a new NHS number and the further development of existing patient databases held by Family Health Service Authorities.

(i) *The Confidentiality of Health Information*

In my last Report I referred to a draft code of confidentiality of personal health information which I suggested might form the basis of a statutory strengthening of the Data Protection Principles in respect of medical confidentiality. The Department of Health had not supported the introduction of a statutory code and was working on draft non-statutory guidance. I have now been in contact with the Minister who has kindly explained in some detail his Department's view of the way in which the common law duty of confidentiality applies to personal health information held for the advice, treatment and health care of patients and for related management purposs within the NHS.

I am considering how the common law duty bears on the application of the Data Protection Principles. However, I remain as yet unconvinced that the common law provides as good a constraint on the use and disclosure of personal health information as could be provided were there to be appropriate statutory provisions. In the absence of statutory provisions I am still awaiting the opportunity to comment on the data protection implications of the Department's non-statutory guidance. I understand that there is likely to be consultation on the Department's view shortly.

The need for guidance can only become more urgent as the extent to which patient information is used in the NHS increases. In this connection I welcome the intention of the NHS Management Executive to issue a code of practice on confidentiality in the contracting environment. I look forward to commenting on the draft of this shortly. This particular code concerns itself principally with the security of personal health information.

The Eighth Data Protection Principle requires data users to take "appropriate" security measures. In the NHS such measures must necessarily be appropriate to the sensitivity of patient information. With the increased flow of patient data associated with contracts there is some evidence that an appropriate level of security is not always achieved. An example is the use of open fax systems to transmit computer generated, named patient information. This matter will be picked up through the report referred to in the introductory remarks above. On a more simple level, I welcome steps being taken by health authorities to send out appointment details in sealed envelopes rather than on postcards.

Drawing the best from these various governmental and health service initiatives should underpin the confidence which the public undoubtedly displays in the confidential treatment of personal health information.

(ii) *Obtaining Health Information Fairly*

The increasing use of computers in the Health Service adds to the importance of ensuring that information is fairly obtained from patients. This is required by the first Data Protection Principle. The significance of

"fair obtaining" is further increased by pressures to share information both within and outside the NHS. These pressures may arise, for example, from links with local authority social services departments arising from the growing emphasis placed on care in the community. Discussions with the Scottish Health Service have led to the development and trial of a system for notifying patients of uses to which their health data may be put. I now hope to extend this activity into England, Wales and Northern Ireland.

A significant source of patient information for the NHS is the patient/general practitioner contact. I am considering the extent to which the general practitioner obtaining information from a patient is required to notify the patient about the way in which that information is used elsewhere within the NHS. I am also 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.

(c) Local Authorities and Schools

(i) *The Council Tax*

The Local Government Finance Act 1992 established a new system of finance for local government known as the Council Tax. The tax will be based in part on property values. The Inland Revenue is already well advanced with the task of compiling lists which put properties into valuation bands.

During the passage of the legislation I expressed concern to the Department of Environment that such lists might be seen by some organisations, particularly those involved in the profiling of individuals for marketing purposes, as a valuable supplement to their existing databases. I was therefore encouraged to see the Government take the view that, as a matter of policy, copies of the lists would not be available for sale commercially. Officials at the Department of the Environment have since provided assurances that mechanisms will be put in place to ensure that neither local authorities nor the Valuation Office Agency will be able to provide information from the valuation lists for non-council tax purposes.

The timetable for introducing the new tax is extremely restricted. Nevertheless it is important for local authorities to take time to consider the requirements of the Data Protection Act when planning their information gathering and handling policies. I very much welcome the early discussions that have taken place between my staff and officials from the Department of the Environment, the Welsh Office and the Local Authority Associations with a view to producing detailed guidance for local authorities.

It is already apparent that the Data Protection Principles will have a particular bearing on some council tax practices. In many households not all of the residents will be liable to pay the council tax. Therefore, in contrast with its predecessor the community charge, there will be no requirement for local authorities to maintain a general register of resident persons. Some information that was once essential for the community charge may be completely irrelevant to a local authority's new council tax functions. Authorities will therefore have to scrutinise their community charge files to ensure that information is not held for longer than necessary. They will also have to ensure that they do not hold personal data for council tax purposes which is, in practice, excessive.

It seems possible that many authorities will wish to supplement existing records by employing statutory powers to collect further information from property owners and occupiers. This may lead to large scale information gathering exercises. I am anxious that local authorities should be fully

conscious of their duties to obtain information fairly from individuals and to collect and hold only the personal data that are relevant to their task.

The community charge led to many data protection problems and to enforcement actions involving many local government officers. I do hope, in the case of the Council Tax, that due attention is paid to guidance as and when it becomes available. For my part, I will do all I can to help with resolving difficulties which may arise.

(ii) *Housing and Community Charge Benefits*

The way computerised records are used by local authorities to administer government benefits raises a number of data protection issues. Claim forms for housing benefit and community charge benefit are complex documents which elicit a great deal of sensitive information about people's finances and personal circumstances. I have received a variety of complaints from members of the public about these forms. Clearly much of the information is genuinely needed for the proper administration of such benefits, but I am anxious that authorities operating in this sensitive area should fully appreciate the disciplines imposed by the Data Protection Principles.

To this end I issued a consultation paper in August 1991 outlining my initial concerns. The paper questioned whether all the items of data held by local authority benefit departments were relevant to all types of claimant. It also raised questions about the length of time for which data should be retained once a claim had ceased. A further issue was the extent to which individuals supplying information on claim forms should be made aware that, in some instances, the information collected from them may be used for purposes unconnected with their claim or may be disclosed outside the local authority.

Following this consultation, my staff have been engaged in helpful discussions with the Department of Social Security and the Local Authority Associations. I look forward to these discussions producing clear and practical advice for the benefit of practitioners towards the end of 1992.

(iii) *Computing in Schools*

The Data Protection Act places the responsibility for compliance with its requirements on those who control the contents and use of personal data. Personal data may be considered as information about living individuals held on computer. In the case of a local education authority (LEA) maintained school in England and Wales which has such information on computer, control is exercised for the most part at school level. This arises from the distinct statutory responsibilities of the LEA, governing body and head teacher. The result is that many governing bodies and head teachers will have to register under the Data Protection Act as data users in their own right.

My staff have assisted officials of the Department of Education and Science (DES) to draft guidance to clarify the registration requirements for personal data held in schools. The DES and the Welsh Office have now issued this guidance to LEAs and LEA maintained schools. With my staff's assistance the DES is also preparing similar guidance for grant maintained schools.

The supporting mechanisms for organising the necessary registrations by governing bodies and head teachers are well advanced. I have made available

a special registration pack to assist schools and over 27,000 of these have been issued. My staff have dealt with a wide range of enquiries from schools and LEAs and will continue to provide help wherever possible. Space has been taken at two national exhibitions for schools at which I have made detailed advice and assistance available.

There has been some reaction from the education sector against these school registration requirements. Clearly it is not possible simply to ignore the working of the Act as far as schools are concerned. The personal data held by schools should quite properly be subject to the Act's requirements. However, I can understand the concerns expressed about the expense for the education sector of so many separate registrations. I therefore put forward a suggestion to the DES as to how the effects of the schools' registration charges might be alleviated without any significant effect on government expenditure. Whilst the Treasury did not feel able to establish such an arrangement, I have been told by the DES that the cost of registrations has been taken into account in the 1992/3 local government finance settlement.

Guidance from the DES and the Welsh Office has, of course, been directed to the registration requirements for maintained schools in England and Wales respectively. I am now considering the registration requirements in so far as they affect maintained schools in Scotland and Northern Ireland.

Registration at school level has provided me with a welcome opportunity to consider how young people can be educated about the rights and obligations associated with the Data Protection Act and about the wider role of computers in society. As a first step a poster has been designed specifically with schools in mind and has been distributed at appropriate exhibitions. The school curriculum provides opportunities to consider the impact of information technology on society and I am conscious that teachers would find a data protection resource pack valuable in addressing this topic. When funds allow, I hope to make such a pack available. In the meantime I welcome any further suggestions as to how data protection can be incorporated into the teaching curriculum and for other materials that teachers would find helpful.

(d) The Direct Marketing Industry

(i) *The Direct Marketing Association*

This year has seen an important move to rationalise representation of the direct marketing industry. A number of trade associations have combined to form the United Kingdom Direct Marketing Association (DMA). I look forward to a constructive relationship with this new representative body.

(ii) *Obtaining Information for the Third Party List Rental Market*

The advertising and marketing industry appears to accept that customers or enquirers should be told if the information they provide will appear on lists for rental for direct marketing. There has, historically, been disagreement between those representing the industry and myself about the timing of this notification, although many individual organisations have followed my advice. My view is that notification must be provided before the customer or enquirer gives his or her information. Individuals can then, if they wish, opt-out of third party mailings simply by deciding not to do business with the organisation concerned. Industry representatives, by contrast, have taken the view that the "fair obtaining" requirement of the First Data Protection Principle can be satisfied by providing a notification of list rental practices at a later date, for instance with the fulfilment of orders. At this point the organisation in question would allow individuals a period of time to register

an objection. A recent appeal against an enforcement notice (see Section 7) should give the opportunity to test the position under the Data Protection Act before the Data Protection Tribunal.

Outside the precise context of the Act, it now appears that the industry has generally accepted my position, for it is enshrined in the British Code of Advertising Practice which has the industry's support. However, this contrasts with the position the industry has taken in its lobbying for changes in the European Community's Draft Directive on Data Protection (see Section 2). Its stance here would weaken the protection for individuals given by the British Code of Advertising Practice and the United Kingdom Act.

(iii) *The British Code of Advertising Practice*

The British Code of Advertising Practice "Rules for Direct Marketing including List and Data Base Management" was launched in January 1992. It is managed by the Advertising Standards Authority (ASA) and has the support of the trade associations in the advertising and direct marketing industry.

I welcome this initiative by the ASA which is designed to be supportive of the Data Protection Act and indeed requires compliance with the Act. The Code supports my view of the "fair obtaining" requirement of the Act and in some ways goes further than the Act. The voluntary pressures applied by the ASA Code should assist compliance with the Act and help to avoid complaints from individuals.

(iv) *Lifestyle Databases*

My staff continue to monitor the compilation and use of large marketing data bases, in particular, the so-called "lifestyle databases" which are built from the responses to mass circulation questionnaires. There are three United Kingdom companies involved in this activity and their databases contain between 1.5 and 3.5 million records. During the last year, it has become clear that it is not only these companies which use the information provided. Particular questions on the survey forms are sponsored by other organisations who themselves make quite extensive and independent use of the information. It appears to me that individuals should be aware of this fact when they complete the survey forms. Agreement has so far been reached with one of the lifestyle database companies whereby there will be an extensive revision of future survey forms. As a result, those completing these forms will be considerably better informed as to who will be holding personal data about them and why.

(e) The Mail Order Industry

I am pleased to have reached agreement with the Grattan group of companies on the "fair obtaining" of information. However, it is not proving easy to get the mail order industry as a whole to adopt the good practices I believe are required by the Data Protection Act. For some time, my staff have been seeking to reach an agreement with the Mail Order Traders Association (MOTA) on the "fair obtaining" of information. The discussions are making slow progress. It is unclear whether the MOTA will be willing to advise its members to meet the standards laid down in the British Code of Advertising Practice referred to above.

(f) Code of Banking Practice

A Code of Banking Practice ("Good Banking") was published in December 1991. It was produced by a Working Group of the Association for Payment

Clearing Services, the British Bankers Association and the Building Societies Association. There was widespread consultation on initial and revised drafts of the Code, before the published version was finalised. The Working Group sought my comments and I was pleased to discuss these at a number of meetings.

The Code is a response to the report of the Review Committee on Banking Services Law (the "Jack Committee") which was published in February 1989. The Committee proposed standards for obtaining, using and disclosing information on individuals which are very supportive of data protection objectives. They concerned, for example, the fair obtaining of information from individuals and practices for notifying individuals of their rights under the Data Protection Act. The Government gave its views on the Jack Committee recommendations in a White Paper. It wished to see its conclusions introduced through a voluntary code of practice for banks and building societies.

I welcome the concern shown in the Code of Banking Practice for the confidentiality of information about individuals. In particular, the restatement of the traditional rules of a banker's duty of confidentiality; the requirement for the express consent of the customer to the disclosure of personal details to third parties for marketing purposes; and the opportunities to be provided to customers to decide whether they wish to receive marketing literature. The Code also refers to the Data Protection Act directly, placing an obligation on banks and building societies to explain to customers that they have a right of subject access under the Act.

An Independent Review Committee has been set up by the three associations named above. It will review the working of the code, consider complaints about breaches of the code and promote its use amongst banks and building societies. In a news release on 30 April 1992, the Committee announced that 237 banks and 90 building societies had adopted the Code. However, it expressed concern about a number of smaller banks which had not yet committed themselves to the Code.

From a data protection viewpoint, I shall be interested to see the detailed practices adopted by those adhering to the Code of Banking Practice. I will seek to check on the position later this year.

(g) Data Matching

"Data matching" is increasingly a subject of discussion and regulation in a number of countries. In Appendix 1 I briefly describe data matching and consider the claims made on its behalf and the countervailing criticisms of it. Following this, I consider the regulation of this technique by the Data Protection Act and actions taken in other countries. My objective is to introduce this subject prior to undertaking a consultation later this year on what might be appropriate policies and rules to govern the use of this technique.

Data matching is the computerised comparison of two or more sets of records. The objective is to seek out any records which relate to the same individual. Where this is such a "match" then the information from one set of records may be transferred to enhance the other set. Alternatively, the information on the matched individual may be extracted for decision and action and may form the basis of a further set of records. This new set may ultimately form a set of "profiles" of individuals drawn from a number of different sources. There is usually the common point that the sets of records being searched have been assembled for different purposes than that which is the object of the data matching.

Data matching has raised concerns in a number of countries and some have taken actions to regulate it. In the United States a "Computer Matching and Privacy Protection Act" was introduced in 1988. In Canada, the Federal

Government has a policy on "Data matching and Control of the Social Insurance Number". This policy incorporates checks by the Privacy Commissioner. In Australia, data matching is covered in the 1988 Privacy Act and the Privacy Commissioner has issued guidelines for its regulation.

I drew attention to the need to consider the issues raised by data matching in my Sixth Report, presented to Parliament in July 1990. The matter was subsequently discussed at a meeting with the Home Affairs Committee of the House of Commons on the 24 October 1990. The Committee recommended that there should be clear procedures governing the merging of files of data. The Government response made clear that it would consider any recommendation on data matching made by my Office.

I propose now to take up the Government's invitation, but first it will be sensible to obtain views from other interested parties. During the next few months my staff will draw up a framework of policies and practices which might be introduced where data matching is proposed. I hope to undertake some consultation on these towards the end of this year.

Meanwhile, it is interesting to see the trends which might lead to the greater adoption of data matching in the United Kingdom. These include the options for collecting census statistics which are currently being assessed and the increasing pressure to make public files available for private use.

(h) The Population Census

The Census Offices of the United Kingdom have recently sought comments on the way the census should be conducted. I was pleased to be asked to give my views and welcome the way in which the Census Offices are openly canvassing opinions on what can be a sensitive subject.

For one hundred and fifty years, the census has been conducted every ten years by means of questionnaires completed by each household in the country. These surveys provided the basis for the statistical information on population and housing on which much public planning depends. The Census Offices' review aims to establish whether any other approach to the collection of information would give better value.

Several of the options put forward for consideration would involve the accumulation of data collected for various different purposes. Among the possibilities canvassed are a 'census via administrative records', which envisages the bringing together of data from different sources through the use of personal identifiers so that a secondary "census" record is created. A further possibility mooted is of establishing links between census and other records. Such options clearly involve data matching and give rise to the concerns that I have referred to above.

A further possibility advanced is the creation of registers of housing and population. It would seem appropriate that any decision to establish such registers should be subject to wide public debate. There should be properly argued justifications as to why such registers should be established and as to where the balance should lie between administrative need and convenience and the interests of individuals. Such registers may also raise wider issues as to the matter of personal identification numbers. Clearly such registers would also attract the attention of commercial and other interests. If they were to be established then it would seem desirable that specific legislation should regulate the form, nature, and use of such registers to ensure appropriate safeguards for individuals.

The Census Offices are also seeking views on the possibility of devolving the collection of census type information to local bodies or separate service

organisations. The consultation paper states that "a move towards a demand-led supply of the information could require a central organisation only as a regulatory body enabling service organisations to compete to meet the specific needs of users". There is a danger that such a development could lead to a dilution of the scrupulous concern for confidentiality that the Census Offices have traditionally displayed.

This is only the first phase of the consultation. I am pleased that the Census Offices will be circulating a summary of the responses before selecting a short-list of options for the future. This will ensure a further opportunity for comment on such potentially significant developments.

(i) The Pressures on Public Information Files

I have welcomed Ministers' decisions not to allow other uses of certain public files: in the past the Community Charge Register; in this Report, the Council Tax Valuation Lists.

However, the pressure to make other uses of public files continues. Some of this pressure arises from public sector bodies who are themselves pressed towards greater commercialisation. In this year, for example, I have received complaints about the use by the BBC of statutorily obtained lists of TV renters and purchasers; and about the Driver and Vehicle Licensing Agency's mailing out of information about a driving school with provisional licences. I have also been approached by one or two commercial concerns worried about the purchase and use of their share registers for direct marketing.

These forms of public information may not be subject to the good practices generally required by the Data Protection Act. This is because information which must be published by statute is not subject to the Act. Also, information which is obtained under statute is deemed to be obtained fairly regardless of the knowledge of the person providing it. However, as mentioned in connection with data matching, I am also looking at the lawfulness of using information, obtained under statute, for purposes other than the one for which it was obtained.

I will take particular cases up with Government departments and others as they arise. In this respect I have been pleased at the positive and helpful response of the Vehicle Inspectorate which is considering the commercial exploitation of some of the information it collects. The Inspectorate has agreed that, where personal data are involved, it will give individuals an opportunity to opt out of the use of their information for marketing purposes.

(j) Uses of the Electoral Register

Last year I referred to a scheme being prepared by the Home Office to encourage Electoral Registration Officers (EROs) to publish a list of those who had bought their registers. This followed a suggestion I made to the Home Office Minister. I am pleased that the Home Office was able to introduce such a scheme in time for publication of the 1991 Register of Electors.

The scheme relates to non-electoral purchasers of copies of the register, either in data form or in hard copy which will be converted into data. Such purchasers are asked to complete a form giving their name and address, indicating which part of the register they are purchasing and describing their reasons for purchasing it. From these forms, EROs compile a list of the information provided which is available for consultation at council offices. The list enables individuals to trace who has purchased information about them and thus to use their rights under the Data Protection Act to check on the subsequent holding and use of their details.

The Home Office scheme only extends to England and Wales. The Scottish Office has now issued a circular initiating a similar scheme for Scotland to be introduced during 1993. Whilst these schemes are voluntary I am encouraged by support given by the local authority associations. I hope to monitor the way in which the Home Office scheme is working during this coming year.

(k) Telecommunications

One telecommunications subject has come increasingly to the fore in the last few years. This is the technique known as calling line identification (CLI). The technique allows a person receiving a telephone call to read, from a display on the instrument, the telephone number from which the call is being made.

The main justification put forward for this technique is that it gives the opportunity to trace nuisance calls. In addition, that it allows a person receiving a call to determine whether to answer it or not on the basis of the calling number displayed. The technique also aids direct marketing by allowing commercial organisations to capture enquirers' telephone numbers.

The argument about nuisance calls is one that appeals, but does not fully stand up to scrutiny. It should be feasible to store all calling numbers at the exchange for a limited period of time to allow a check to be made following, for example, a complaint to the police. Procedures are, in any event, already being introduced to trace nuisance calls. On the other hand, it seems wrong that a person making a telephone call should not have some control over whether his or her location is revealed or not.

Matters have advanced furthest in the United States, where there have been differing responses to CLI. Some States have declared CLI unlawful, others allow it, others demand safeguards. The position is not yet resolved in the United Kingdom, but discussions are taking place between the telephone companies, the Office of Telecommunications and the Department of Trade and Industry.

I have produced a brief paper on CLI which has been fed into these discussions. A copy of the paper is in Appendix 2. The paper shows how the Data Protection Act applies to CLI and concludes that telephone callers should generally have a free and simple method of blocking the use of this technique.

4 Credit Reference and Third Party Information

This year has seen the final stages of a long-running dispute I have had with the finance industry. The dispute began with complaints I received from individuals even before the Data Protection Act came fully into force in 1987. Previous Annual Reports have told the story as it has unfolded. This Section brings together the main points of the story, details the conclusions of the Data Protection Tribunal and looks to future effects and actions for individuals and the credit industry.

(a) Background

There are four major credit reference agencies in the United Kingdom. The practice of these agencies is to extract information from their files on the basis of the addresses at which a credit applicant lives or has lived. They then supply details of all the persons recorded at those addresses to an enquiring lender. This information about people other than the applicant is referred to as 'third party information'.

The result is that lenders are provided with information on third party individuals who may have nothing to do with the applicant, or with his or her ability or intent to repay the loan requested. Nevertheless, lenders may use this third party information to determine whether the applicant should receive a loan or not.

Individuals have regularly complained to my Office about the effects of this practice. The complaints illustrate that the practice can have outrageous results. Individuals have been refused credit on the basis of bad debts of other people who may simply have chanced to live at the same address at some time in the past.

In May 1988 I invited representatives of the finance industry to meet me to discuss this and other issues. Following this meeting the finance industry formed a Data Protection Forum and towards the end of 1988 presented me with a report supporting the extraction and use of third party information. The report suggested some changes which the industry felt it might be able to make.

Whilst all sections of the industry were represented on the Forum and were apparently parties to the report, the mail order industry asked for a separate meeting with my Office to put its views. This was held in December 1988. The mail order industry kindly arranged for presentations explaining the operation of the industry and putting views as to why its position was different from the rest of the finance sector. I was not convinced by these arguments. It appeared to me that the arguments of the various parts of the finance industry were, in substance, the same.

I responded to the Forum in February 1989. I could not accept the arguments of the Forum either at law or as to their statistical soundness. I did not feel that the movement offered by a part of the industry went far enough to remove what I considered to be unfair processing by the credit reference agencies in breach of the Data Protection Act.

In my response, I forecast that I would have to use the enforcement powers of the Act to remedy matters. Nevertheless, I continued to try to resolve matters by discussion and I am grateful for the efforts put into this process by a number of individual members of the Forum. However, we were unable to make any progress. The position taken by the mail order industry and the later repudiation of the Forum's views by a number of witnesses at the Tribunal hearings were particularly disappointing.

As well as discussing the third party information issue I suggested that it would be valuable to look at longer term solutions. My objective was to find some method for credit reference which would meet the needs of the finance industry whilst complying with the requirements of the Data Protection Act. In the event, these suggestions were not taken up.

Therefore, in August 1990, I issued enforcement notices against the four main credit reference agencies—CCN Systems Limited and CCN Credit Systems Limited (these may be considered as one organisation), Infolink Limited, Wescot Data Limited (which later became Equifax Europe Limited) and CDMS Limited. The objective of these enforcement notices was to cause the agencies to extract information from their files on the basis of name and address and not simply address. The notices recognised that some third party information could be relevant to the ability or intent of a credit applicant to repay a loan and it did not preclude the agencies from extracting such information.

All of the agencies appealed against the enforcement notices to the Data Protection Tribunal.

(b) The Tribunal's Hearings and Decisions

The hearings took place during 1991, that concerning the CCN organisations in January, followed by Infolink in April, Equifax in May and CDMS in July.

The Tribunal delivered its judgement in the first case, that of CCN Systems Limited and CCN Credit Systems Limited on 25 February 1991. In this judgement, the Tribunal endorsed my views on the approach to the law and found it was unfair to process personal data as the agencies did. However, the Tribunal considered that a distinction should be made between different types of third party information—in particular information which might be about a member of a credit applicant's family and information which appeared to be about an unconnected stranger. A further concern to the Tribunal was information which might in fact be about the applicant, but which contained a misspelling or variation of his or her name.

In the light of these findings, the Tribunal concluded that I should have exercised my discretion differently with regard to the requirements laid on CCN by the enforcement notice. The Tribunal therefore delivered an amended enforcement notice in which it incorporated its own conclusions. CCN and I both lodged appeals to the High Court against the Tribunal's judgement. A more detailed description of the CCN judgement is given in my last annual report (Seventh Report—June 1991).

The Tribunal's judgement on the three remaining cases followed—on 31 May 1991 (Infolink), on 28 June 1991 (Equifax), and on 15 October 1991 (CDMS).

In each of these cases, the Tribunal's judgement broadly followed the same pattern as in the CCN case. However, a number of additional points or issues under the Data Protection Act 1984 were raised at these hearings and were considered by the Tribunal. These are dealt with separately under 'Advice for Data Users' in Section 5. In all its findings of law the Tribunal supported my views and decisions.

In each judgement, the Tribunal set out its findings, its reasoning and the substance of its decision. However, in contrast with the CCN decision, the Tribunal did not include amended enforcement notices in its judgements. Rather, the Tribunal indicated its intention to deliver amended notices in accordance with its findings. It then adjourned the hearings to a later date so that the parties to the appeals could make representations on the terms of the amended enforcement notices.

The three credit reference agencies and my Office exchanged views on the amended notices, but it proved impossible to agree a form of notice acceptable to all parties which could be put before the Tribunal. I therefore applied for further hearings by the Tribunal to settle the form of notice.

The Tribunal held two further hearings on the form and wording of amended enforcement notices. The first of these, on 12 February 1992 heard submissions on behalf of Equifax, CDMS and myself. The second, on 19 February 1992, heard submissions on behalf of Infolink and myself.

On 28 February 1992 the Tribunal delivered its amended notices in all three cases. The notices were identical. They differed in a number of ways from the amended notice delivered in the CCN case.

I considered the terms of these amended notices and took further advice from leading counsel. I can only appeal against a decision of the Tribunal to a higher court on a point of law. I was advised that such an appeal would be unlikely to succeed. However, it did seem to be undesirable that there should be two different forms of notice applying to the credit reference industry. I therefore reached agreement with CCN Systems Limited and CCN Credit Systems Limited that they would accept a notice in the same form as that delivered in the other three cases. That agreement is awaiting embodiment in a consent order in the High Court which will resolve the outstanding appeals by CCN and myself. Neither I nor any of the other three agencies have lodged appeals against the amended notices issued by the Tribunal at the end of February. These enforcement notices are therefore the final resolution of this matter.

The Tribunal has set 31 July 1993 as the date by which all the agencies must comply with the notices. From this date there will be limitations on the information that the agencies will be able to extract about people other than a credit applicant. This marks a major change in the practice of credit reference in the United Kingdom.

There is now a set of rules governing what information can be extracted by credit reference agencies. The rules are complex and a copy of the Tribunal's final enforcement notice is given in Appendix 3. This Appendix also gives the names and addresses of the four credit reference agencies against which I took action.

The following seeks to describe the practical effects of the rules from the notice:

1. Agencies may not supply information from their files on any person who does not live or has not lived at the same address at the same time as the credit applicant.

   Bearing in mind this limitation, then:

2. Agencies can supply information from their files where the information matches the name and address of the credit applicant either by a match on surname only, or by a match on both surname and on forename or initials. Agencies can also supply information where the name on the files is sufficiently similar to the credit applicant for it to be reasonable to believe the information to be about the applicant. However, the agencies cannot supply information in either of these categories where it is reasonable to believe that it does

not refer to the credit applicant, for example a difference in sex is implied by the title used.

3. Agencies can supply information from their files where the information shows a different surname from the credit applicant if the agency knows beforehand that it refers to the applicant, eg. a woman who has changed her name on marriage.

4. Agencies can supply information from their files about other people than the credit applicant as long as those others have the same surname and it is reasonable to believe that they have been living, at some time, as a member of the same family as the applicant in a single household. This also applies where the surnames of the other people are sufficiently similar to the credit applicant's for it to be reasonable to believe that they are the same.

5. Agencies can supply information from their files about other people who have different surnames from the credit applicant as long as they know facts beforehand which support a reasonable belief that they have been living at some time as a member of the same family as the credit applicant in a single household.

6. Agencies *cannot* supply information from their files about any other person, even if it would fall into categories 4 or 5 above if the agency has information from which a reasonable person would believe there is no financial connection between the credit applicant and that other person.

(c) The Effect of the Tribunal's Judgement on Individuals

The good news for individuals is that, from 31 July 1993, the Tribunal's enforcement notices preclude the credit reference agencies from extracting information on individuals who have not lived at an address at the same time as the credit applicant. I am pleased that the Tribunal has supported me so as to get rid of a totally unfair and unacceptable credit industry practice—extracting information on people the credit applicant has never lived with, or perhaps even known. This should avoid a problem for many thousands of individuals in the future.

However the Tribunal's notices do generally allow the agencies to continue extracting information on other individuals who are reasonably believed to have, at any time, lived at the same address as the credit applicant as a member of the same family in a single household.

There may be difficulties for individuals in this second aspect of the Tribunal's judgements. For example, a credit applicant may not have lived with, or even seen a member of his or her family for many years. Nevertheless, if that family member has had a county court judgement against him or her at any time, the agencies may supply details of this to lenders as relevant to the credit applicant's ability or intent to repay the loan for which he or she is applying.

About one in three of the complaints received by my Office concerns consumer credit. A proportion of these complaints has always related to 'family' information, where the credit applicant was refused credit because a member of the family had incurred debts of which the applicant knew nothing and for which the applicant had no responsibility. I have now established a system for recording the proportion of new complaints of this nature and will monitor trends in these.

A recent complaint illustrates the issue. This was from a lady who, although she had properly repaid credit on several occasions herself, had an application for credit refused. The credit reference agency had provided information to the lender on the bad debts of a son who had left home seven years previously. The

debts had been incurred after he had left home. The lady was given to understand that these debts had been taken into account in the credit decision.

The Tribunal accepted my arguments that individuals should be able to guard themselves against the circumstances in which this lady found herself. They can do this by taking advantage of rule 6 in the above list. This stops agencies extracting information about other people, even members of the same family, where the agency knows there is no financial connection between the two.

An individual who may wish to apply for credit can notify the credit reference agencies if he or she is financially independent, or if there are people in the family with whom there is no financial connection. The agencies may wish to make some enquiries or checks to ensure that such an individual is not trying to avoid a bad credit record. However, unless the agencies have some reason to doubt the good faith of the individual it seems to me that they must act on the information they have been given.

A way forward for individuals may be to write to the credit reference agencies and obtain a copy of their file, which they are entitled to do under the Consumer Credit Act. The process is simple, involving only a written request and an enclosure of £1. The addresses of the relevant agencies are given in Appendix 3. An individual's file will show whether there is information on other people whose financial circumstances will not affect his or her ability or intent to repay a loan. If the file contains information on people who have no financial connection with the enquirer, then this should be made clear in writing to the agency concerned.

It is important that individuals are informed about the new credit reference rules laid down by the Data Protection Tribunal. In particular they will need to be made aware of the important opportunity to set right false assumptions of financial connections with other individuals. A major part of my efforts over the past years has been to increase public awareness of individuals' rights in respect of information. It is very unfortunate that this new requirement for public education should have coincided with a cut in the grant-in-aid allotted to my office.

My Office is writing to all those who have complained about the use of third party information. The letter informs these individuals of the position following the Tribunal's judgements and advises them of their new rights. However this initiative can only reach to those who have complained.

(d) The Effect of the Tribunal's Judgements on the Credit Industry

The credit reference agencies have until 31 July 1993 to bring their systems into line with the enforcement notices issued by the Data Protection Tribunal. From the evidence given at the Tribunal hearings, the changes may well be significant and costly.

The new rules laid down by the Tribunal will not only affect the credit reference agencies, but also many lenders and the credit scoring systems they employ. They may also affect procedures followed by the Office of Fair Trading (OFT). I am making arrangements to discuss matters with the various parties concerned so as to ensure that there is a common understanding of future requirements.

The Home Affairs Committee of the House of Commons expressed a particular interest in the results of the Tribunal appeals and, through this Report, I am briefing the Committee on them.

5 Appeals heard before the Data Protection Tribunal

The Registrar does not determine the meaning of the law. That is a matter for the Courts. However, as Registrar, I do have to take a view of the way in which the Act applies to the many and varied circumstances in which personal data are held used and disclosed. These first views are stated generally in the Guideline Series. The Guideline booklets contain advice for data users on the meaning and application of the Data Protection Act 1984. They are available, free of charge, from my Office.

If there has been a contravention of the Data Protection Principles, I may issue a supervisory notice against a data user to put matters right. The data user can appeal against a notice to the Data Protection Tribunal.

An appeal to the Tribunal against a decision of the Registrar may be on the facts; the law; the exercise of the Registrar's discretion; the terms of the notice served by the Registrar; or the time in which the notice is to take effect. The Tribunal may uphold or overturn the notice served by the Registrar or substitute any decision or notice which could have been made by the Registrar.

The Tribunal may hold a hearing to determine an appeal or may proceed on the basis of written representations. In proceedings before the Tribunal it is for the Registrar to satisfy the Tribunal that the disputed decision should be upheld. After every case the Tribunal gives a written decision setting out its findings and the reasons for its decision.

Beyond the Tribunal, either the appellant data user or the Registrar may appeal to the higher courts on points of law. It is here that the meaning of the law is finally determined.

The Tribunal sat on six occasions during the year. Five of these were in connection with the appeals by the credit reference agencies. The result of these appeals is reported in Section 4. On the sixth occasion, the Tribunal convened to consider an appeal by the Halifax Building Society. This section deals with this appeal and also contains advice for data users arising from all the Tribunal's decisions. Information on appeals awaiting hearing by the Tribunal is given in Section 7.

(a) Appeal by the Halifax Building Society

In January 1992 the Tribunal was convened to hear an appeal by the Halifax Building Society (the "Society"). This was against an enforcement notice alleging that the Society had failed to satisfy the right of an individual to have a copy of the information held about him or herself by the data user. This is known as the "subject access right". The appeal did not proceed to hearing but was settled by an agreement between the parties which was placed before the Tribunal.

The complaint leading to this appeal had been long-running. The complainant had applied to the Society in November 1987 for a copy of the information held about him. He had not been satisfied that he had received all he was entitled to and complained to my Office in December 1987.

Meetings and discussions with the Society produced more information which I considered should have been given to the complainant. The Society argued that certain categories of information could be regarded as system security data and could be withheld from an individual under the "crime prevention" exemption in section 28(1) of the Act. This exemption allows the withholding of information in any case in which its provision would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. There was no suggestion that the complainant was in any way untrustworthy or dishonest. I issued an enforcement notice in respect of these categories of information in February 1989. The Society appealed against this notice to the Tribunal.

I later issued a preliminary notice in respect of further information. A preliminary notice is a forewarning that an enforcement notice may be issued. It gives the data user the opportunity to make representations against this. The Society provided the further information in dispute but did not accept my view that it was personal data which the Society was obliged to provide under the subject access right. As the information had been provided I had no power under the Act to pursue this matter any further. However, the Society's response meant that the issue was left outstanding since the Society might withhold this information from individuals seeking to exercise their subject access rights in the future.

Shortly before the hearing of the appeal in January 1992 I reached an agreement with the Society under the terms of which I withdrew the enforcement notice. The terms of this agreement are in Appendix 4. Through the agreement the Society undertook that, in replying to future subject access requests, it would give individuals all the categories of information which had been provided to the complainant in this case. This included those categories given as a result of the preliminary notice. It also agreed that if, in future, the Society withheld information in reliance on the "crime prevention" exemption it would notify individuals of this fact. It would also inform them of their right to complain to the Registrar and would provide further information if an individual complained or enquired about particular transactions. The Society also conceded some of its arguments of law but both parties reserved their positions of law in respect of the "crime prevention" exemption.

I concluded that the agreement achieved more for individuals as a whole than pursuing the enforcement notice to its conclusion. It also left me free to pursue any future action I thought appropriate in the event of other complaints. The Tribunal noted and lent its support to the agreement. The complainant expressed satisfaction with the outcome.

(b) Advice for Data Users

At the start of this Section I explained that I publish advice to data users through a series of Guideline booklets. In last year's Report, in order to help data users, I extracted the more general points of law from the decisions made by the Tribunal and cross referenced these to the Guidelines. Again this year, I have been pleased that the Tribunal's views on the law have supported those taken by my Office and contained in the current Guidelines. However, the Tribunal sometimes expands on the Guidelines and the following points have been noted from this year's Tribunal decisions.

1. In considering whether processing is fair or unfair there may be many ways in which it may be unfair. The concept of unfairness is not a limited one (Guideline 4, pages 6-12).
2. In assessing "fairness" under the First Data Protection Principle, while paramount consideration is to be given to the interests of the individual data subject, not the data user, 'paramount' does not bear the meaning that this is the only consideration, but rather the most important single consideration. This is a development by the Tribunal of its view given in

last year's Report on page 21, point 3. (Guideline 4: page 4, Introduction, lines 5-10; page 8, paragraph 1.4, lines 1-2; page 11, paragraph 1.10).

3. Under the Act, processing of personal data is defined to include the extraction of the information constituting the data. In determining that processing has taken place in this way, it is not necessary to show that the use of the information has been completed, or that the information has been seen by a human being. Information may be extracted at a stage before a human being actually sees the information. (Guideline 2, page 14, paragraph 7.2).

4. Section 28(4) of the Act exempts personal data from the Registrar's powers to take enforcement action by reference to the First Data Protection Principle. This is not a blanket exemption but is limited to particular cases in which such action would be likely to prejudice the purpose set out in section 28(1): the prevention of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty (Guideline 4, page 12, paragraph 1.12).

5. Section 1(7) of the Act determines that personal data are only processed (and therefore caught by the Act) if any of the operations which constitute processing are performed "by reference to the data subject". If the object of the processing is to learn something about the individual the data will be processed by reference to the data subject even if the enquiry has not been made using the name of the individual (Guideline 2, page 14, paragraph 7.3).

6 Complaints from Individuals

The number of complaints received this year from individuals has fallen to 1747 from the 2419 received in the previous year. Some indication that there are latent, untapped, data protection complaints came following an interview I gave on the "Help Squad" ITV programme. Despite individuals having to use teletext to find out the Office address and telephone number, over 400 people contacted the enquiry service within two or three days of the programme. Following this, the rate of receipt of complaints more or less doubled for the next two or three weeks. The key problem therefore seems to be to get an informed and educated public. I return to this in Section 9.

Complaints about unsolicited mail have fallen steadily in numbers and as a proportion of complaints received over the last three years. They now account for only 18.5% of the complaints I receive as opposed to the 44.5% reported in my Sixth Annual Report (June 1990). Consumer credit complaints remain at around 32% of all complaints. I am unclear as to what will happen to this type of complaint in the light of the Data Protection Tribunal's enforcement notices against the credit reference agencies (see Section 4). These notices come into force on 31 July 1993.

This year there have been 65 complaints about non-registration. This amounts to some 4% of all the complaints I have received. It is disturbing to find that individuals are continuing to find organisations that are not registered under the terms of the Data Protection Act 1984. Although I have prosecuted a number of companies for non-registration, in the past this action has normally been the result of my own investigative work rather than as a result of complaints.

Complaints about the First Data Protection Principle and, in particular about the unfair obtaining of personal data have risen in numbers as compared with last year. Complaints about the subject access provisions of the Act remain steady at about 200 per year. Some organisations, when receiving subject access requests, do not always seem to be able to handle these adequately. Some appear not to have established subject access procedures at all. Complaints jolt these organisations into setting up systems to deal with these requests.

My Office still deals with 36% of all complaints completely within three months and 67% within six months. However, the remainder can take some considerable time to resolve.

Some examples of complaints are:

Case 1

A telephone company asked the complainant for a deposit for £200 before installing a telephone in her home. The company had stated that she was a bad credit risk after referring to a credit reference agency.

There was no adverse information on the complainant's credit reference file. However the file did not show her name as listed on the electoral roll although the complainant said that her name should have been on the register from the previous April. The complainant had written to the telephone company enclosing a copy of her driving licence and her tenant's agreement.

The telephone company was asked for its comments. The reply stated that a misunderstanding had taken place between the company and the complainant concerning the contents of her credit reference file. The request for the £200 deposit was dropped and the complainant was provided with a telephone service.

Case 2

The complainant received mail in an envelope with three windows. It could be clearly seen that he held an account with a particular bank. He objected to this disclosure of information and did not want to receive any further promotional mailings from the organisation concerned.

The organisation suppressed the complainant's details so that he would not receive further mailings. As a direct result of this complaint the data user also discontinued the use of that type of envelope for direct mail promotions.

Case 3

The complainant did not receive a reply to his subject access request. The data user, a football association, was approached and subsequently a response was sent to the complainant. The data user also agreed to implement new procedures for dealing with these requests.

Case 4

The complainant received an Income Tax Notice of Coding which bore the name of a company for which he had never worked. However he had worked for a company with a similar name and he complained that this company had passed information on to the company named on the Notice of Coding.

The investigation revealed no evidence that any information had been transferred from one company to the other although it transpired that the same people had been involved in running both companies.

The tax office concerned had the same reference for both companies. However both references were now historical records and the complainant's tax records were corrected.

Case 5

The complainant had her community charge paid for her on two occasions by someone she did not know. She had complained to the Council after the first occasion. After the second occasion she complained that the Council had contravened the Data Protection Act by disclosing information about her to the unknown "benefactor".

The Council gave assurances that the person already knew the information required to make the payment. The complainant was advised but she felt that this information could only come from the Council's records.

The Council's registration for the Collection and Recovery of Community Charge was thoroughly checked and it was felt that even if details of the complainant's account had been disclosed, it would be open to the Council to argue that the disclosure was covered by this registration.

Case 6

There were a number of inaccurate entries on the complainant's credit reference file. The credit reference agency corrected most of the inaccuracies. There was however, one particular entry relating to a default, which the agency seemed unable to amend. Some times the default was shown as "unknown" and at other times the default was shown as £99,998. Investigations revealed that the inaccuracies kept recurring due to a systems error. The credit grantor had informed the agency many times to amend the entry. The agency agreed that, to prevent the balance of £99,998/unknown being restored, it would set up a balance of zero and delete the entry.

Case 7

The complainant was a taxi driver who had been licensed by the local Council for the last five years. Subsequent to getting his licence the complainant was taken to court for minor charges.

In 1990, the Council established a system whereby all new taxi drivers and all those renewing all existing licences would have to make a subject access request to the police under the provisions of the Data Protection Act to obtain details of any convictions held against them. The response from the police was to be delivered in a sealed envelope to the licensing office of the Council.

When his licence was due for renewal the complainant made a subject access request to the police and handed the response to the licensing office.

Subsequently, at a public meeting, a document was circulated by the Council which listed details of the previous convictions of taxi drivers whose licences were not renewed because they had not declared their convictions in the previous years. The list gave the initials of the taxi drivers and details of their convictions.

The Council stated that the details of the convictions, as received from the police, were not computerised and therefore the disclosure at the public meeting was not of personal data covered by the Data Protection Act. However, as a result of discussions with the Registrar's Office, the Council agreed that, in future, to preserve the anonymity of the taxi drivers concerned, they would not use initials but only case numbers.

Case 8

The complainant had a County Court Judgement entered in his name. Details of this judgement appeared in his credit reference files. He told the credit reference agencies that the judgement related to a claim resulting from a motoring accident which his insurers had paid belatedly. The agencies refused to remove the judgement and suggested he added a Notice of Correction. The complainant asked the Registrar for help in removing the judgement.

The credit reference agencies were advised that they were contravening the Fourth Data Protection Principle by holding this judgement on the complainant's file since it was irrelevant to the purpose of assessing his credit-worthiness.

All the agencies agreed to remove the entry.

Case 9

A trade union official complained on behalf of his members who were working in a local authority Treasurer's Department. The complaint concerned the checking of personnel records against community charge records to see if employees living

within the local authority's boundary were (a) on the Community Charge Register and (b) up to date with their community charge payments. One member of staff had been found not to be registered and had been suspended from work.

It was discovered that manual personnel records only were being used and no computer records were created or amended during this activity. The complainant was told that there was no further action that the Registrar could take.

Case 10

The complainant received an electricity bill for a property that was not his. The property in question was for sale through agents and the complainant's sister owned a flat adjoining it. The complainant believed that the electricity company had assumed that the property concerned was part of his sister's flat. All the bills for the sister's flat were sent to her at her home address except the community charge bill which was sent to the complainant. He believed therefore that the only organisation which could have provided his name and address in connection with the disputed property was the Community Charge Department of his local authority.

The complainant informed the electricity company that he had no connection with the address on the bill he had received from them. In spite of this he received another demand some time later. This time he complained to both the electricity company and to the Registrar.

The electricity company was unable to say from exactly where it had obtained the erroneous information that the complainant was responsible for this electricity bill. It amended its database, apologised and offered compensation.

Case 11

The complainant had received several items of mail from a clearing bank addressed to a Mr X at the complainant's address. Unwilling to open someone else's mail the complainant returned the mail to a local branch of the bank and explained that he had no knowledge of Mr X.

Later the complainant began to receive letters from a debt collection agency, also addressed to Mr X. He complained to the Registrar. After contacting the bank concerned, the complainant received an apology and an assurance that the bank would review its procedures to try to prevent a similar mistake from happening in the future.

Case 12

The complainant continued to receive bills from a newsagent after he had cancelled his order and the shop had stopped delivering papers to him. Despite several requests the bills continued to arrive. The complainant made a subject access request to the newsagent and complained to the Registrar. As a result of contacting the newsagent the complainant received an apology.

Case 13

The complainant received a registration document for a car which he did not own. He wrote to the Driver and Vehicle Licensing Agency (DVLA) telling them of this mistake. However, he later received a parking ticket for the vehicle concerned. He complained to the Registrar. Investigations revealed that someone with a similar name and address to the complainant was actually the registered keeper

of the vehicle. The complainant received a full explanation and apology from DVLA.

Case 14

The complainant had booked a holiday in the United States. With the confirmation of her flight booking she also received a computer-produced list of the names and addresses of her fellow travellers. The complainant was unhappy with the security implications of this list. She wrote to the Registrar.

It was discovered that the travel agent concerned was not registered to hold personal data. The travel agent registered and now only circulates names and addresses of passengers with their written consent.

Case 15

The complainant was concerned about the positioning of a VDU screen at her local newsagents. The screen was on full display to customers in the shop. The complainant was particularly concerned because a lot of elderly people live in the area and paid their paper bills in the newsagents. Their addresses were being disclosed to other customers and individuals in the shop at the time.

The newsagent was told of the need to register and of the requirements of the Act in relation to the security of data. He immediately repositioned the VDU.

Case 16

The complainant had been refused credit on the basis of information on his credit reference file relating to someone with a different name who used to live at an address close to his own.

The bank concerned was unable to trace the source of the error, but contacted the credit reference agency to ensure that the details were corrected and erased from the complainant's file.

Case 17

Two doctors who had set up a new partnership after dissolving their previous partnership complained about their former partner. They were concerned that their former partner was still holding data about their patients and was sending unsolicited letters to them.

The former partner was advised that in holding information about these patients he was contravening the Fourth, Fifth and Sixth Data Protection Principles. He undertook to delete the information in question. He had previously written to the patients to explain the circumstances leading to the break-up in the partnership and agreed not to contact these patients again.

Case 18

The complainant wrote to the Registrar after receiving a large amount of unsolicited mail. Because of the way in which his address was formatted he believed that the source of his details was a weekly magazine to which he subscribed.

The publishers of the magazine arranged to suppress the complainant's details on lists which they intended passing on to other organisations for mailing purposes.

They were advised how to make an amendment to their register entry in order to cover themselves for this list rental activity. They had previously sent in the forms to do this but had completed them incorrectly and had not responded to correspondence from the Office.

Following this visit the publishers failed to submit the necessary amendments. The register entry for the publishers also expired. A renewal was not submitted and the organisation was prosecuted under Section 5(1) of the Data Protection Act for holding personal data without being registered. The company pleaded guilty and was fined £160 and ordered to pay prosecution costs of £340.

Case 19

After having made a subject access request to his local Health Authority, the complainant claimed that the information forwarded to him made no mention of treatment he had received in 1984, and that many of the codes used were unexplained.

The Health Authority stated that the complainant had received all the relevant information held about him. The reason that the details relating to his treatment in 1984 were not shown was because the computerised Patient Administration System did not come into operation until 1985. They also sent the complainant further explanations of the codes used, and were advised that, in future, individuals making subject access requests should be provided with these additional explanations.

The complainant was advised that if he wanted to obtain information that may have been held in manual form he should either contact the health care professionals he consulted at the time, or approach the contact at his local hospital who was responsible for the Access to Medical Records Act.

Case 20

The complainant claimed that a cheque for £1,000 that had been paid into his current account had been cleared according to his local branch. After he withdrew the money he was told that the bank had made a mistake, the cheque had bounced and he now owed £951 to his account. The debt then showed up on his credit reference file, but related to a credit card account. This was incorrect as the debt related to the complainant's current account. The bank insisted that the debt of £951 still stood and would not be removed from the complainant's credit reference file.

The question arose as to who was liable for the debt, as the bank claimed that the complainant still owed it the money, while the complainant argued that the debt was only incurred because of the bank's error.

The Registrar took the view that if the bank was not entitled to claim repayment, then the data would be inaccurate and should be deleted. If the bank was entitled to repayment, but the complainant disputed his liability for the debt, then it would seem, under a Minute of Understanding between the Registrar and the major banks, that the information should not have been disclosed to the credit reference agency.

The Registrar also pointed out that the bank has discretion as to which debts are disclosed to the credit reference agency, and taking into account the bank's error and the question of who was liable for the debt, it was suggested that the bank removed the disputed entry.

The bank agreed that due to the particular circumstances it would remove the entry in the credit reference files, but insisted that it was still entitled to repayment of the debt.

Case 21

Details of a loan account in the complainant's name were disclosed to her husband. He was seeking financial advice from a Branch Manager of the bank and was not previously aware of his wife's loan.

The complainant had already approached the bank and the member of staff had been made aware of the seriousness of the complaint. All staff at the branch have been advised of the importance of the bank's duty of confidentiality to their customers.

Case 22

An elderly lady tried to rent a television set but was refused by the television rental company. When the lady obtained a copy of her credit reference file, she saw that there was adverse information concerning a County Court Judgement shown on it. This judgement related to an individual at her neighbour's address.

The lady's daughter asked us to investigate. It was discovered that the judgement relating to the neighbour's address had been incorrectly registered at the elderly lady's address.

Registry Trust, which holds records of County Court Judgements, corrected its records as did the credit reference agencies.

Case 23

The complainant had initially been working from home for his employer. The employing company was responsible for the payment of his telephone bill and this was sent directly to it.

The complainant then started to work from his employer's office and asked the telephone company to send bills to his home address as all calls on the subsequent bills would be personal. When he later reverted back to working at home he had a private line that was not funded by his employer.

However, the employing company had contacted the telephone company requesting that future bills be sent to them to process in the previous manner. An employee of the telephone company assumed that it was the complainant who had made this request and did not make a thorough check on the identity of the caller. The bills were then sent to the employing company. Normally a bill would not have been sent directly to an employer without the express consent of the private line customer.

The telephone company admitted that there had been an unauthorised disclosure of information and apologised for any inconvenience caused. It offered the complainant an ex-gratia payment of £100, which was accepted. For the future, it was agreed that all requests about the direction of bills to the employer would be made in writing to avoid a similar mistake.

Case 24

After the complainant's husband's death her solicitor sent the premium bonds found in his papers to the Bond Office. Although some of the bonds were in her late husband's name, there were others which were not. The complainant was not sure if they were hers or her late husband's. The Bond Office advised the solicitors that one of the bonds did not belong to either husband or wife.

The complainant wrote to the Registrar (nearly four years after her husband's death) as she felt that she may have lost prize money and, she said, she had not even been repaid the cost of this bond.

The Bond Office advised that it did not keep any computerised information about the complainant's husband since it was more than three years since his bonds had been encashed. It also found the application form for the disputed bond clearly showing the name of the person making the application and the name of the Post Office where the application was made. It was not made out in the name of the complainant's husband.

Case 25

The complainant received a questionnaire through the post and was concerned about the security of any information supplied. More generally, she objected to the receipt of unsolicited mail.

The company responsible for the survey was in the market research industry and was a member of the appropriate trade associations. It advised that any personal data supplied by a member of the public, would be held in a confidential manner and would not be disclosed to any third parties; it complied with its trade association's codes of practice.

The company explained that the complainant's details had been obtained from an organisation that held a computerised version of the electoral roll. This organisation suppressed the name and address of the complainant on its files.

Case 26

The complainant objected to the receipt of unsolicited mail. On contacting the organisation which had mailed her she was advised that her details had been obtained in a mailing list from a ticket booking agency, which the complainant recognised as one from whom she had purchased cinema tickets.

The booking agency's entry on the Data Protection Register had expired prior to the complainant purchasing her tickets. The agency was prosecuted for not being registered and fined £250 with £100 costs.

Case 27

A couple were refused credit and obtained a copy of their files from the credit reference agency. They found a number of items relating to another family with the same surname who lived in the same village but a different street.

The couple contacted their solicitor and their MP, who both took up the matter for them. The organisation from whom they had sought credit apologised and made a compensatory payment.

The MP was dissatisfied with the credit reference agency's response and contacted the Registrar. This case will now be resolved in the light of the recent decision by the Data Protection Tribunal on the extraction of third party information from credit reference agency files.

Case 28

The complainant wrote to the Registrar concerning the receipt of unsolicited mail addressed to her 11 year old daughter. The mailing advertised the products

of a well known brand of cigarettes. The complainant stated that she lived in a no-smoking household.

The tobacco company traced the name and address to a holiday competition entrance coupon available in many pubs and bars; the form clearly was aimed at smokers. The complainant did not recognise the handwriting on the coupon and therefore it would appear that she had been the victim of a hoax.

The tobacco company removed the daughter's details from its database.

Case 29

The complainant was refused a further advance on his mortgage. The credit grantor advised him that the advance was refused due to a County Court Judgement registered at his address in a very similar sounding name to his own. The complainant was aware that one of his neighbours did have a similar name to his, and, on obtaining a copy of his credit reference file, he found that the judgement information related to his neighbour.

The plaintiffs in the judgement case were traced through the Courts. The plaintiffs stated that, due to a typographical error, the summons was issued against the complainant's address rather than that of his neighbour. Arrangements were made by the plaintiffs to have records amended at the Registry Trust Limited.

In the meantime the credit grantor concerned was made aware that the judgement had incorrectly been registered at the complainant's address. The credit grantor agreed to give the credit facility required by the complainant.

Case 30

A complaint was received from a small publishing company regarding the unfair obtaining of a copyrighted directory list by another organisation. There were certain clearly defined restrictions concerning the use of this information. Because these restrictions were not adhered to, unsolicited mail was sent out by the organisation complained about. Complaints were then received by the publishing company from people who had received the mailings.

The publishing company approached the other organisation and was informed that no further mail would be sent. However two years later more mail was sent so the matter was brought to the attention of the Registrar.

The organisation carrying out the mailings was advised that not only was the information obtained ignoring a copyright warning, but also the data was retained when it was irrelevant to the marketing activities concerned and kept for longer than necessary. The organisation deleted the information from its files.

7 Enforcing the Act

It may be helpful to remind readers that enforcement actions can be of two kinds:

— prosecutions for offences flowing, for example, from contraventions of the Act's registration requirements. Most of these cases are triable in either the Magistrates' or Crown Courts, or their equivalent in Scotland and Northern Ireland. They have usually been heard in the Magistrates' Court.

— supervisory notices, which are designed to set right contraventions of the Data Protection Principles. The Principles set out the good practices with which data users must comply. There are three types of supervisory notice—Enforcement, De-registration and Transfer Prohibition Notices. The Registrar may also refuse a registration application. These notices may be appealed to the Data Protection Tribunal.

(a) Prosecutions

Charges have been brought this year under the following sections of the Act:

Section 5(1): Holding personal data without being registered or without having applied for registration. (Data Users who fail to renew their register entries are also charged under this section).

Section 10(9): Failure to comply with an enforcement notice.

Prosecutions have been brought against 27 data users for criminal offences under the Act and a further 8 are awaiting hearing. The cases which have been concluded are listed in Table 1.

Table 1: Prosecutions in the Year to 31 May 1992

Section of the Act	Data User	Court	Date	Fine £	Costs £
5(1)	Spacetime Systems Ltd	Bow Street	19.06.91	250.00	100.00
10(9)	CCRO—Suffolk Coastal District Council	Woodbridge	01.08.91	Acquitted	
5(1)	Allstarr Video	Harrow	15.08.91	250.00	250.00
5(1)	Batricar Ltd	Bow Street	02.09.91	200.00	200.00
5(1)	Teamstrike Ltd	Keighley	06.09.91	250.00	170.00
5(1)	Greystone Leisure Ltd	Keighley	06.09.91	250.00	170.00
5(1)	Harold Haynes t/a Videoscene	Solihull	18.10.91	Absolute Discharge	50.00
5(1)	RM Information Consultants Ltd	Old Street	30.10.91	500.00	250.00
5(1)	International Society for Krishna Consciousness Ltd	Watford	12.11.91	1000.00	717.56
5(1)	J R Philips & Co Ltd	Bristol	18.11.91	200.00	120.00
5(1)	Cotton Traders Limited	Trafford	19.11.91	200.00	150.00
5(1)	Cotsworld Travel Ltd	Gloucester	13.12.91	400.00	100.00
5(1)	Neil's (London) Ltd	Harrow	28.01.92	250.00	200.00
5(1)	Kevin David Cripps t/a Kavern Records and Video	Chester	30.01.92	100.00	200.00
5(1)	G A Property Services Limited	City of London	13.03.92	500.00	500.00
5(1)	Ashton Drake Galleries Limited	Harrow	24.03.92	750.00	350.00
5(1)	Turner Recruitment Ltd	Cambridge	30.03.92	200.00	100.00
5(1)	Mark Quibell t/a Quill Business Publications	Birmingham	06.04.92	Conditional Discharge	25.00
5(1)	Raymond Orrell t/a Financial Advice Bureau	Houghton le Spring	24.04.92	100.00	250.00
5(1)	Wersi Electronic Organs and Pianos (UK) Ltd	London	28.04.92	50.00	150.00
5(1)	Dodd Marketing Ltd	Harlow	29.04.92	400.00	300.00

Section of the Act	Data User	Court	Date	Fine £	Costs £
5(1)	Learned Information (Europe) Limited	Oxford	30.04.92	500.00	500.00
5(1)	Photosol Limited	Basildon	05.05.92	150.00	350.00
5(1)	Roger Leslie Cartwright	Bristol	14.05.92	150.00	120.00
5(1)	The Home Shoppe Ltd	Richmond	18.05.92	1,750.00	1,100.00
5(1)	Bowker Direct Marketing Limited	Bridgnorth	18.05.92	100.00	150.00
5(1)	Carlton Brookes Limited	Dudley	20.05.92	Conditional Discharge	125.00

So far there have been no prosecutions of directors or employees of data users although such individuals have responsibilities under the Act, breach of which may constitute a criminal offence. During this year I had occasion to consider the prosecution, under Section 5(2)(d) of the Act, of an employee. The employee had gained access to the employer's computerised customer records, in order to pass on details of a customer to her friend, for use for her friend's own purposes. The employee had been given instructions about her responsibilities under the Act.

The incident highlights the fact that employees should be aware that, if they make an unauthorised disclosure of personal data, they may be committing a criminal offence for which they can be prosecuted personally.

In this case, I took into account the fact that the employee concerned was asked to resign as a result of the incident and I did not proceed to a prosecution. Having made this position public, I do not undertake to follow this course in the future.

(b) Supervisory Actions

This year has seen a development in the use of formal undertakings to resolve matters where I consider that a data user is in breach of a Data Protection Principle. These undertakings extend the practice of resolving issues by discussion, whilst still avoiding the necessity to resort to formal supervisory action. The undertaking is a formal document which sets out the issues which have been considered and the steps which the data user has agreed to take to ensure compliance with the relevant Data Protection Principle in the future. It is signed on behalf of the data user by a senior officer of the organisation and a record of it is retained in my Office. The undertaking is so designed that I may take action on it in the future if the data user fails to meet its terms.

Preliminary notices have been served on nine data users: Following representations five of these cases have been resolved by the organisations concerned giving formal undertakings to amend their procedures and practices. These organisations are: John Govett Unit Management Limited; Kaleidoscope Limited; Hope Mail Order Limited; Aspect (Mail Order) Limited; and Page and Moy Limited.

Three of the preliminary notices have led to formal Enforcement Notices against: Consumerlink Limited; Trent Mail Order Company PLC and Innovations (Mail Order) Limited. One preliminary notice is still in the period allowed for representations. This is against G.U.S. Mail Order Limited.

A further five formal undertakings have been given without the service of preliminary notices. The organisations giving these undertakings are: Grattan Plc; Look Again Limited; You and Yours Limited; Streets of London Limited; and Sophistique Designs Limited.

All except one of these actions and undertakings relate to the direct marketing or mail order industries and are concerned with the fair obtaining of information.

One hundred and thirteen Registration Refusal Notices have been served on individuals, companies and other organisations, (eg. schools and voluntary groups) where inadequate information had been provided on the application for registration. One preliminary notice of intent to refuse registration was served but following discussions with the data user the difficulties were resolved.

(c) Appeals to the Data Protection Tribunal

Information on appeals heard during the year is given in Section 4 (re the credit reference agencies) and Section 5 (re the Halifax Building Society).

Five appeals are awaiting hearing by the Tribunal. Two appeals are against enforcement notices served in respect of the fair obtaining requirement of the First Data Protection Principle. These have been brought by Consumerlink Limited and Innovations (Mail Order) Limited. Three appeals are against refusals of registration.

(d) Monitoring and Promoting Compliance with the Act

(i) *Obtaining and using Information for Direct Marketing*

In my last Annual Report I described a project for monitoring "off-the-page" advertising which appeared to seek information about individuals that might subsequently be held on computer. The objective is to determine whether advertisers are appropriately registered. Where advertisers rent enquirers' and customers' names and addresses to other companies, there is also a check that the advertisers obtain their information fairly by notifying individuals of this fact before they provide their information.

In the last year, my staff have initiated enquiries regarding 203 advertisers. In 17% of cases it appears that advertisers did not computerise details of respondents to their advertisements. In about a further 25% of cases it was found that advertisers were correctly registered and obtaining that information fairly in accordance with the First Data Protection Principle. Investigations are still continuing, and so far there have been 8 prosecutions for non-registration. The checks so far seem to indicate issues of compliance with registration or with the Data Protection Principles in almost half the cases sampled.

In January 1992 a second project was initiated. Data users, whose lists are advertised as available for rental by third parties, are sent a letter setting out their legal obligations in terms of registration and the fair obtaining of personal data. They are asked to complete a short questionnaire designed to establish the nature of their rental lists and elicit the steps they have taken to notify individuals of the rental information they have provided. It is too early to report on the findings of this exercise in detail. However, preliminary results suggest that only about half of the companies concerned may conform, in all respects, to the registration and fair obtaining requirements of the Act.

(ii) *Meeting Registration Requirements—the "Town Test"*

The objective of a "town test" is to encourage registration of data users in a particular area. This is achieved by a variety of activities such as distributing explanatory leaflets, and by random visits by investigating staff to a range of different organisations. These activities take place over about two weeks during which time efforts are made to obtain supportive media publicity.

The first of these town tests was held in Cambridge in May 1991. That was reported last year. A second town test was held in early November 1991 in Stockport. Here, activities were extended by a stand at the local business show and by running two well attended seminars.

These town tests do result in an increase in registration applications and a further test has just taken place in Dundee. This follows the appearance

at the Scottish Computer Show. Unfortunately, some organisations choose to ignore advice to register and some prosecutions have followed as a result.

(iii) *Checking those who fail to renew registrations*

As indicated in Section 8, a substantial proportion of data users fail to renew their registrations when they expire. It seems clear that this can occur because many smaller firms go out of business. However, investigations so far have shown that there are others, perhaps as many as 14% of those who fail to renew who should re-register. Some have sought to say, in their defence, that they did not receive the renewal reminders by virtue of their having moved address. But, failure to ensure an entry contains a registered persons's current address is also an offence and prosecutions for non-renewal can be expected to continue.

8 The Data Protection Register

This has been a busy year. On 1 June 1991, that is at the very beginning of the year under review, the registration fee increased from £56 to £75. Advance publicity announcing the increase had resulted in more than 4,000 applications for registration and more than 3,500 requests to renew entries being received during May 1991. This meant that the year began with a backlog of applications awaiting processing. During the year itself, more than 16,500 applications for registration were received. In addition there have been around 22,000 requests to amend entries on the register.

Despite these heavier than expected volumes, the processing backlog has been reduced and all outstanding refusal cases have been completed. At the end of the year there were 164,500 entries on the Register.

A new contract has been negotiated for the computer bureau processing of the Register for the next three years. The revised contract offers considerable scope for savings when compared with earlier years but does require closer scrutiny of the flow of processing each month. Costs have also been reduced by some detailed changes to the computing system during the year.

The work load in the coming year will be extremely heavy. This is because of the cyclical nature of registration renewals. A peak of second renewals will occur during summer 1992 as a result of the large number of entries which were added to the register during the middle of 1986.

From the renewal requests received so far, it seems that the proportion of organisations not renewing at the second renewal stage (ie. 6 years after acceptance onto the register), is likely to be at least as high as the proportion not renewing at the first renewal stage. This is of concern not only from a financial point of view and because of the extra work involved in the follow-up but because of the implication that a number of data users are breaking the law. A follow-up is now done where entries are not renewed and a number of prosecutions have been brought, and are continuing to be brought, where evidence is found of organisations failing to renew when registration is required. This topic is also touched on in Section 7.

9 Informing People about the Act

In a number of places in this report I have referred to the importance of informing people about the Act. There is a massive awareness task to be carried out, both for individuals and for data users. It is with considerable concern and regret therefore that, in seeking to trim sails to cater for a cut in grant-in-aid in the 1992/1993 financial year, I have been compelled to make severe reductions in this activity. There will be little finance for other than imperative updating of such as the Guidelines and I see no realistic possibility of any significant advertising expenditure. I shall be curtailing appearances at exhibitions and have taken steps to reduce external public relations expenditure.

(a) Strategy

During the 1992-93 year, I will seek to optimise the distribution of information materials already to hand. It will be important to get the maximum help from others in holding or distributing information on the Data Protection Act. Resources permitting, fresh approaches will be made to organisations such as the Citizens Advice Bureau and bodies representing small firms. An initiative was taken last year to brief solicitors and accountants so that they can advise their clients and an attempt will be made to build on this. I will seek to continue the initiative to support schools and other educational establishments, for I feel that this is sowing the seed corn for the future.

(b) Activities

For some years I have sought to target data users and data subjects equally through promotional activities. Resources have not allowed that this year and progress has once again been heavily reliant on public relations activities and a generally reactive rather than proactive approach.

One small advertising campaign was conducted during the year. Using the theme 'Ignorance is no Defence', it was directed towards reminding professional advisers (solicitors, accountants, management consultants) of their clients' need to register under the Act. Advertisements ran in the business journals for these professions in the early part of 1992. The advertisements incorporated a response coupon to enable advisers to send for a special information pack and to indicate an interest in future data protection training programmes.

A leaflet has been produced giving a very simple introduction to the Act and its associated rights and obligations, as a first step for those whose knowledge of the Act is minimal. This leaflet ('What is Data Protection?') incorporates a tear-off card for those wanting further information. More than 40,000 of these leaflets have been distributed resulting in requests, in particular, for registration packs and the Guideline booklets. A large poster and some small 'reminder' stickers about data protection have also been produced to tie in with the leaflet. These have all proved to be popular, particularly at exhibitions.

In March 1992, all registered data users and computer bureaux were sent a new edition of the data protection newsletter 'Update'. This once again incorporated a poster directed at compliance with the Data Protection Principles. At the same

time, a new publication was produced ('Now you're registered: a guide to your obligations under the Data Protection Act') which will in future be sent to all data users when they are notified of their acceptance onto the Register. There are details in this publication of a 'commitment statement' which can be used by any organisation which is confident it is complying fully with the Data Protection Principles and can demonstrate this if challenged. The statement will hopefully meet a need which has in the past been expressed to my Office by a number of organisations.

Demand for existing publications continues to be high with over 31,000 sets of Guidelines distributed during the year and 40,000 registration packs. A special registration pack for schools was produced in response to the recent requirement for school governors and head teachers to register. Over 27,000 of these packs have been issued, together with more than 7,000 copies of a Guidance Note on the subject. There have been 21,718 requests for the rights leaflet for individuals ('If there's a mistake on computer about you').

A new promotional venture has been the production of a fifteen minute video introducing the Act. Known as a 'video brochure', it is a text-driven production using library footage and stills as a relatively inexpensive means of producing what is traditionally a very expensive promotional item. Final modification to the video brochure should be completed shortly and it will then be distributed as an educational and training tool.

In June 1992, staff gave a further series of one-day seminars for the advertising and marketing industry. The seminars were again set up in conjunction with a professional seminar company and were well supported by representatives from a wide range of organisations.

The Office took stands at 15 different shows throughout the country. These ranged from large computer shows, to small regional business exhibitions and those concerning a particular business or professional sector. A small travelling exhibition stand has been purchased with the intention that this should be made available for unmanned exhibitions and for displays in libraries and similar venues.

Throughout the year, the Office issued 24 news releases on a variety of activities and issues. There were over 1,500 press mentions, 16 radio interviews and 7 television appearances. My appearance early this year on a national prime-time consumer affairs television programme, discussing the Act and the rights it bestows upon individuals, resulted in over 400 enquiries to my Office. This served as a powerful reminder of the direct and important relationship between media activity and complaints and registration numbers.

This year staff have given 54 talks to a wide variety of audiences. A more pro-active approach has been taken to supporting training for individual organisations and representative bodies, through the provision of speakers and training material. The effectiveness of this will be monitored, as will the demands on staff time.

As always, the Enquiry Service had a busy year, dealing with some 39,261 telephone calls and 13,338 letters. Total enquiries have been exceeded only in the initial registration year of 1985/86. Considerable work has been done to match the provision of telephone enquiry lines to the pattern of demand during the day and throughout the week. This has resulted not only in a better service for enquirers, but has enabled more enquiries to be handled without increases in cost.

time, a new publication was produced ('Now you're registered: a guide to your obligations under the Data Protection Act') which will in future be sent to all data users when they are notified of their acceptance onto the Register. There are details in this publication of a 'commitment statement' which can be used by any organisation which is confident it is complying fully with the Data Protection Principles and can demonstrate this if challenged. The statement will hopefully meet a need which has in the past been expressed to my Office by a number of organisations.

Demand for existing publications continues to be high with over 31,000 sets of Guidelines distributed during the year and 40,000 registration packs. A special registration pack for schools was produced in response to the recent requirement for school governors and head teachers to register. Over 27,000 of these packs have been issued, together with more than 7,000 copies of a Guidance Note on the subject. There have been 21,718 requests for the rights leaflet for individuals ('If there's a mistake on computer about you').

A new promotional venture has been the production of a fifteen minute video introducing the Act. Known as a 'video brochure', it is a text-driven production using library footage and stills as a relatively inexpensive means of producing what is traditionally a very expensive promotional item. Final modification to the video brochure should be completed shortly and it will then be distributed as an educational and training tool.

In June 1992, staff gave a further series of one-day seminars for the advertising and marketing industry. The seminars were again set up in conjunction with a professional seminar company and were well supported by representatives from a wide range of organisations.

The Office took stands at 15 different shows throughout the country. These ranged from large computer shows, to small regional business exhibitions and those concerning a particular business or professional sector. A small travelling exhibition stand has been purchased with the intention that this should be made available for unmanned exhibitions and for displays in libraries and similar venues.

Throughout the year, the Office issued 24 news releases on a variety of activities and issues. There were over 1,500 press mentions, 16 radio interviews and 7 television appearances. My appearance early this year on a national prime-time consumer affairs television programme, discussing the Act and the rights it bestows upon individuals, resulted in over 400 enquiries to my Office. This served as a powerful reminder of the direct and important relationship between media activity and complaints and registration numbers.

This year staff have given 54 talks to a wide variety of audiences. A more pro-active approach has been taken to supporting training for individual organisations and representative bodies, through the provision of speakers and training material. The effectiveness of this will be monitored, as will the demands on staff time.

As always, the Enquiry Service had a busy year, dealing with some 39,261 telephone calls and 13,338 letters. Total enquiries have been exceeded only in the initial registration year of 1985/86. Considerable work has been done to match the provision of telephone enquiry lines to the pattern of demand during the day and throughout the week. This has resulted not only in a better service for enquirers, but has enabled more enquiries to be handled without increases in cost.

11 International Activities outside the European Community

International interest in data protection continues to grow. To some extent this is driven by developments in the European Community (EC), particularly in connection with the draft directive on data protection. EC matters are dealt with in Section 2. Here I look at other international activities with which my Office has been involved.

(a) The Council of Europe

Twelve countries have now ratified the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Finland having done so in 1991.

During the year the Committee of Ministers has approved a recommendation on the protection of personal data held in public files. The Project Group on Data Protection has prepared a recommendation on the protection of personal data in telecommunications which is awaiting the approval of the Committee of Ministers. A further working party has begun consideration of data protection in respect of census and statistical data.

The Working Group on Medical Data has developed a draft recommendation for appropriate safeguards for personal health information and is now turning its attention to genetic information. I anticipate that the Group will present its draft recommendations later this year and that, in due course, a new recommendation will be approved by the Committee of Ministers to take the place of the existing recommendation on medical data banks, dating from 1981.

My staff attend the meetings of the Council of Europe Project Group on Data Protection and the Working Group on Medical Data.

(b) The International Meeting of Data Protection Commissioners

In 1991 this took place in Strasbourg to mark the tenth anniversary of the Council of Europe Convention. Discussion was concentrated on developments in the Council of Europe and in the European Community. This meeting marked the first occasion on which there were official representatives from the United States. In all, some twenty-nine countries sent delegates or observers.

The Working Party on Telecommunications and the Media has met twice in the last year, in Berlin and Brussels. Its work has in the main concentrated on the issues raised by the draft recommendation on telecommunications of the Council of Europe and the European Community Draft Directive on Data Protection in Telecommunications.

(c) Other International Contacts

The Fourth Global Congress on Patient Cards in Berlin in May 1992 included a session devoted to privacy and data protection implications. My Assistant Registrar who is responsible for liaison with the Health Sector attended. One of my staff attended the OECD Ad Hoc Experts Meeting on Data Privacy Protection held in Paris. My Senior Assistant Registrar attended a briefing meeting on the Schengen Information System in Brussels.

Two meetings of the British Data Protection Authorities (Guernsey, Jersey, the Isle of Man and the United Kingdom) were held during the year; in the Isle of Man and in Wilmslow.

My Office has this year received visitors and delegations from Czechoslovakia, Germany, Guernsey, Hungary, Israel, Japan, Jersey, Isle of Man, the Netherlands, New Zealand and Uganda.

Once again I record my gratitude for the cooperation and assistance I have received from the Data Protection Authorities of other countries.

12 Organisation and Finance

(a) Organisation

For some years my staff have been housed in two separate buildings. During this year the lease for the smaller premises fell due for renewal. This coincided with the availability of new premises, located within a few hundred yards of the previous main office, which would house all the staff. It was possible in the current economic climate to negotiate favourable terms for release of the previous leases and for entry into the new premises. The move, bringing all staff together in one building was made in April 1992.

(b) Level of Grant in Aid

The amount of grant-in-aid for the year to 31 March 1993 has been set at a lower level than last year and represents a reduction of 6.2% in real terms. This is despite the fact that, in this current year, the Office faces the peak of the three year cycle of registration renewals and an influx of new registrations from schools.

Nor do the signs for the future look auspicious as the proposals I made last year for the Treasury three year public expenditure survey received little or no recognition. Based on the present Treasury proposals my Office is scheduled for a shortfall in forecast necessary grant-in-aid of 23.1% in 1993-94, 15.9% in 1994-5 and 23.4% in 1995-6.

Last year I accepted that difficult financial situations can arise from time to time when commenting on a grant-in-aid lower than proposed; this year I must express real concern. A principal effect of the cut-backs in grant-in-aid is to undermine the education and awareness activities aimed at both the general public and data users. But there are also question marks over my ability to deal properly with registration work. The die is now cast for this year, but the future remains fraught.

(c) Results for the Year

Expenditure for the year at £3.40M was £22k less than the amount budgeted. Receipts from registration fees amounted to £2.25M. In addition, a further £170k was received from a variety of sources including interest earned on funds in hand. An unaudited financial statement is in Appendix 6. The full audited account will be certified by the Comptroller and Auditor General and laid before Parliament later this year as required by the Act.

13 Conclusions

The Council of Europe Convention on Data Protection and associated national pieces of legislation arose from concern in the sixties and seventies about human rights and the burgeoning power of computers and communications. The Convention relates this to the privacy of individuals. It seeks to offer individuals some protection in circumstances where information about them is used by others.

There can be no such thing as absolute individual privacy. Balances need to be struck between the right to privacy and other public objectives. Thus, privacy will be challenged by the need for national security; for financing the nation; for a healthy population; for protection against crime; and by the rights and freedoms of others. The Convention recognises this.

As we go into the nineties, the automation of information handling continues apace. Much of that information is about individuals. Developments outlined in this and earlier Reports suggest that the concerns about privacy expressed in the sixties and seventies will be writ large in the coming years.

In this Report I refer to developments in both the public and private sectors which involve assembling and processing massive collections of information on people. Some of those collections are now looking to extension across the European Community. I also note pressures to use information held in public files and the consultation by the Census Offices on the possibility of drawing together information from many sources and of creating a population register.

I have commented in previous years on policies, such as common systems for identifying individuals, and on technologies, such as improved communication systems, all of which foster the automation of information. This year I review the issue of data matching—bringing together information on individuals which may have been gathered by different data users for disparate purposes. I suggest a need for policies and practices to govern the use of this technique.

The Data Protection Act introduced measures of protection for individuals which have enabled the United Kingdom to ratify the Council of Europe Convention. However, unlike the Convention, the Act does not refer to privacy, it is simply a statute "to regulate the use of automatically processed information relating to individuals . . .". On the other hand, the European Community Draft Directive on Data Protection is concerned with privacy and, in its initial form, gives greater control and greater protection to individuals than the Act.

The first version of the draft directive is not perfect and some changes in it are to be expected. But changes may be crucial to privacy and data protection in the United Kingdom for the foreseeable future. Will the draft directive retain its initial strengths and meet its objective of setting a high standard of protection for individuals in Europe? Much will hang on discussions over the next twelve months, on the reactions of the European Parliament and, ultimately, on the decisions of the Council of Ministers.

Without adequate protection there is a grave danger that individual privacy will simply be whittled away.

Eric Howe
Data Protection Registrar
June 1992

Appendix 1

Data Matching

"Data matching" is increasingly a subject of discussion and regulation in a number of countries. This paper briefly describes data matching and considers the claims made on its behalf and the countervailing criticisms of it. Following this, it considers the regulation of this technique by the Data Protection Act and actions taken in other countries.

(i) *What is Data Matching?*

Data matching is the computerised comparison of two or more sets of records. The objective is to seek out any records which relate to the same individual. Where there is such a "match" then the information from one set of records may be transferred to enhance the other set. Alternatively, the information on the matched individual may be extracted for decision and action and may form the basis of a further set of records. This new set may ultimately form a set of "profiles" of individuals drawn from a number of different sources.

There are a number of variations of the technique. For example, records on a single or a selected number of individuals may be sought from a particular file. Alternatively, a set of records may be searched to find all those with a particular set of characteristics. However there is usually the common point that the sets of records being searched have been assembled for different purposes than that which is the object of the data matching.

There have been some significant comments related to this area from the Judiciary. In a judgement delivered in November 1990, when considering the powers of the police to disclose information obtained using compulsory powers, Vice Chancellor Sir Nicholas Browne-Wilkinson, the senior judge in the High Court Chancery Division, observed that: "if the information obtained by the police, the Inland Revenue, the social security services, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state".

Justice La Forest of the Supreme Court of Canada has stated that: ". . . if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. . . . Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated".

(ii) *The Claims for Data Matching*

Discussions in other countries have led to a number of benefits being claimed for the use of data matching. They include:

— detection and deterrence of fraud or other irregularities, for example, fraudulent or multiple claims, unreported income or assets, impersonation;

— verification of information supplied;

— verification of eligibility, for example for a benefit programme;

— identification of corruption or mismanagement, for example, conflict of interest; unusual payments; excessive withdrawals;

— construction of comprehensive databases for research purposes;

— identification of suspects through searching on the basis of the characteristics of potential offenders;

— improved efficiency, for example, in identifying and concentrating on genuine beneficiaries; or locating and rectifying discrepancies and errors;

— cost effectiveness.

(iii) *The Criticisms of Data Matching*

As benefits have been claimed, so there have been balancing criticisms of data matching. They include:

— lack of a general government or public oversight;

— cost/benefits are not thoroughly analysed so as to properly justify data matching programmes;

— poor quality and inaccurate information leads to mismatches and the replication of errors;

— information is used out of context and may be untimely, insufficient, or unsuitable for the purpose of the match;

— information flowing from matching should be properly verified;

— machines should not be used as substitutes in qualitative decision making for human discretion and judgement;

— the assembling of new files of profiles of individuals leads to the replication of inaccuracies and the drawing of what may be unjustifiable conclusions;

— individuals lack knowledge and control over the use of information about themselves;

— data matching constitutes a "fishing expedition" without any pre-existing evidence or suspicion of wrong-doing;

— a presumption of innocence is turned into a presumption of guilt;

— individuals are not given any adequate opportunity to contest the results of a "match";

— profile searching in particular results in a mass or class investigation, conducted on a category of people rather than individual suspects;

— allowing different organisations to exchange personal data weakens the traditional concerns for confidentiality in each.

(iv) *The Role of the Data Protection Act*

The different techniques which may be adopted in data matching are described above. In each case the records are processed within the meaning of the Data Protection Act. Therefore, any data user wishing to employ these techniques must ensure he is complying with the Act.

Clearly there may be registration requirements and these should be borne in mind by the data user. However, this paper looks more specifically at the requirements of the Data Protection Principles. The use of data matching without sufficient safeguards carries with it serious risks of breaching a number of these.

The first Principle requires that personal data shall be fairly and lawfully processed. The Data Protection Tribunal has made clear in its judgements that, in assessing fairness, the position of the individual and the effect of the processing on the individual are of central significance. A matching programme which led to the replication of errors, the mismatch of information or the holding of irrelevant or out of date information, might amount to unfair processing and be in breach of this Principle.

The Second Principle requires that personal data shall be held for one or more specified or lawful purposes. It seems most likely that public files will be used for data matching. Those files will have been obtained and will be held by a public body for purposes which that body has a statutory duty to carry out. It is not necessarily open to such a body to use and apply such information for other purposes. The public body may be placed under restraints upon its powers under the general law. In some circumstances it may be unlawful for information obtained under statute and held for one purpose to be used for other purposes. Leading counsel's opinion on these issues is being sought.

Data matching leads to the use of information for different purposes than that for which it is primarily held. On the face of it, this calls into question the issue of compatibility raised by the Third Data Protection Principle. This Principle states that personal data shall not be used or disclosed in any manner incompatible with the purpose for which they are held. However, the interpretation to this Principle effectively negates its requirement for it allows any uses and disclosures of personal data providing they are registered.

The Fourth, Fifth and Sixth Data Protection Principles are concerned with the quality of personal data. They require that they should be: relevant and not excessive; accurate and, where necessary kept up to date; held no longer than necessary. These requirements, other than being accurate and being up to date, relate to the purposes for which the personal data are held.

Personal data which has been collected by different data users for different purposes may well contain elements which are, for example, irrelevant to each others' purposes or inadequate for those purposes. The Registrar's Office has encountered significant problems already with the use of information collected and generated for one purpose and its application in another context. These have occurred in the case of the use of County Court Judgement records by credit reference agencies. In these cases efforts are made by the agencies to ensure that the information is accurately matched and attributed to the correct individual and the correct address. However, the quality of the Judgement information makes it difficult to achieve this and it is a continuing source of concern. This reference to the quality of the Judgement information does not imply that it is inadequate or insufficient to the purpose for which it is originally held, but that there are difficulties in attempting to put it to another use.

(v) *The Position in Other Countries*

Data matching has raised concerns in a number of countries and some have taken actions to regulate it. In the United States a "Computer Matching and Privacy Protection Act" was introduced in 1988. In 1989 the Canadian

Privacy Commissioner issued a Directive called "Data Matching and Control of the Social Insurance Number" under the authority of the 1985 Privacy Act. The Directive set out Government policy in this area and gave the Privacy Commissioner express authority to check adherence to this policy. In Australia, data matching is covered by the 1988 Privacy Act and the 1990 Data Matching Programme (Assistance and Tax) Act and the Privacy Commissioner has issued formal binding guidelines for its regulation.

Each of these initiatives allows for some form of overseeing authority and a set of rules which those wishing to carry out data matching must follow. As can be seen from the above, the overseeing authority is usually an independent organisation. In the United States however, each Federal Agency establishes its own Data Integrity Board. This has the perceived weakness of the poacher also being the gamekeeper.

(vi) *Conclusion*

It may now be an appropriate time in the United Kingdom to seek a balance between the benefits which data matching might bring and the privacy of individuals. The balance should be such that, even if it is appropriate to press ahead with a particular application of data matching, there are adequate safeguards for individuals.

Appendix 2

Calling Line Identification

This paper considers the technique known as Calling Line Identification and reaches conclusions about its position in relation to the Data Protection Act.

1. WHAT IS CALLING LINE IDENTIFICATION?

1.1 For the purposes of this paper, what is meant by Calling Line Identification (CLI or Caller ID) is a facility whereby the recipient of a telephone call can see the caller's number displayed from the time that the telephone first rings. It is one of a range of features becoming possible with the modernisation of telephone networks.

1.2 CLI can apply to all calls, including those from equipment with an analogue link to the local exchange, provided that the receiving equipment has the necessary display facilities.

1.3 It mainly benefits the called party in the following ways:—

1.3.1 By partially removing anonymity from those making calls it is likely to reduce the number of malicious calls. (This is borne out by evidence from Canada where investigations of obscene phone calls fell from 322 per month to 83 per month following the introduction of CLI.)

1.3.2 It assists the emergency services in tracing the source of calls, where this is not stated, and would also discourage the number of hoax calls.

1.3.3 It gives the recipient of a call the opportunity to decide, on the basis of the displayed number, whether or not to accept a call.

1.3.4 Transmission of the caller's number creates other possibilities for the called party, such as the capture of the caller's number, and immediate linkage with databases which can provide and capture additional information about the caller.

1.4 CLI has disadvantages for the caller:—

1.4.1 If the display of numbers were compulsory and universal, the ex-directory system would be prejudiced. (It has been suggested in the USA that ex-directory subscribers should display a confidentially registered alphanumeric identifier instead of their phone number. The Federal Communications Commission rejected this proposal as being difficult to operate while offering no unique benefits.) The threat of malicious calls would be reduced, but the number of unwanted calls (eg from patients to doctors at home) could increase as the result of the availability of callers' numbers. (In the USA, commercial companies have set up 'cleaning services' to assist in overcoming this difficulty. Calls are routed through an agency in such a way that there is no means of tracking an individual's calls. This makes telephone records useless to the police, as well as protecting the individual's privacy.)

1.4.2 Compulsory universal CLI would also make the anonymous calling of helplines, or of the police to give information, very much more difficult, restricting such calls to those made from public telephone boxes. It could also be a hindrance to organisations such as the police when making calls as part of their duties, but very restricted exemptions (for a few tightly defined categories of caller) from a general requirement to display the caller's number would not be helpful, as the identity of the caller could still be surmised.

1.4.3 CLI could also lead to increased numbers of 'junk telephone calls', if the numbers of callers to suppliers of goods and services were 'captured' for later marketing use. This has been a particular problem in some States of the USA.

1.5 CLI therefore has benefits for the called party, in providing him with extra information about the caller even before he has accepted the call, but raises the question of how best it can be implemented without enabling the called party to take unfair advantage of the caller.

2. Privacy Implications of CLI

2.1 As noted above, CLI reveals something about the whereabouts and identity of callers and thus may infringe their privacy. In doing so, it makes further infringements more likely in the form of returned calls. The privacy implications are increased if reverse directories, from which subscribers' names and addresses can be obtained by reference to their telephone numbers, are available. British Telecommunication PLC (BT) has no plans to make such directories available in this country, and the Registrar understands that current Department of Trade and Industry (DTI) and Office of Telecommunications (OFTEL) policy is opposed to their introduction.

3. Blocking

3.1 Blocking of CLI is a technically feasible means of mitigating some of the intrusions of privacy caused by CLI. It can operate in three main ways:

3.1.1. *Call Blocking:* This enables the caller to block the transmission of his number each time a call is made. It could be done in a number of ways—for example by pressing a button on the telephone, by dialling a combination of digits before making a call or by asking the operator to block CLI. These are technical decisions, not options available to the individual. Call blocking gives the caller a choice with every call as to whether or not to use it, but such a system of positively opting-out for each call could mean that more vulnerable people, such as the elderly, children or those under particular stress, might be those least likely to remember to operate the blocking system when making a call.

3.1.2 *Line Blocking:* Under this system, the subscriber arranges for CLI to be blocked on all calls from his number.

3.1.3 *As the default system:* CLI would be blocked on all calls unless the caller activated it, whether on a call-by-call or line basis.

3.2 *Block blocking:* This feature would allow a subscriber to refuse to accept calls without CLI. It would be possible to inform a caller of this, to offer him the chance of unblocking CLI and calling again.

3.3 It is possible to give, for example, the emergency services, facilities to override blocking on incoming calls.

3.4 While blocking facilities have obvious advantages for the privacy of the individual, they may reduce the advantage of CLI in deterring malicious callers, as would a system of positively opting-in to CLI. Modern technology, however, retains traces of a call even after it has ended. This permits services such as 'call trace' in the United States allowing the number of a malicious caller to be recorded by the telecommunications operator even when it has not been displayed to the called party. The reception of malicious calls may be further prevented by the use of block blocking.

4. Helplines

4.1 The operation of call blocking should provide privacy for those calling helplines, although the risk remains that the caller may omit to operate the block. Helpline operators could increase privacy by suppressing the receipt of CLI on their apparatus, although callers would need to be convinced that it did genuinely operate. The easy availability of public telephone facilities is an important alternative for helpline callers.

4.2 Calls to anonymous police lines represent a similar difficulty, particularly if blocking on calls to emergency services were automatically over-ridden.

5. Data Protection Implications

5.1 The Data Protection Act covers the type of telephone data under consideration here. Private subscribers' telephone numbers are recorded in a form in which they can be processed automatically and are therefore personal data. They are held by telecommunications operators and the system uses and sends them. They are processed, in the context of CLI, when the caller's number is extracted and is displayed. The systems operator controls such data extraction and is, therefore, the data user. In a system where blocking was an option this would still be the case as the operator would act on the request of the subscriber but would be able to override any such instructions, eg to remove blocks on calls to the emergency services.

5.2 In the terms of the Data Protection Act and in accordance with the line taken by the Registrar over other issues, universal mandatory CLI without blocking would undoubtedly lead to cases of unfair processing, because it would prejudice the ex-directory system and permit the uncontrolled capture of personal data. However, the whole system is not intrinsically unfair in such a way that the introduction of CLI should be opposed, but it is capable of being used unfairly, so that safeguards would be necessary.

5.3 The first of these safeguards would be to make subscribers aware that their numbers would be displayed to called parties. Thereafter, some form of blocking should be available which is easily activated and free to use, ie which offers minimal disincentives to its use. This would give callers the opportunity to ensure that their data were, with possible exceptions (eg emergency services), only displayed with their agreement.

6. International Attitudes to CLI

6.1 Attitudes between, and within, countries with the technology to make the introduction of CLI feasible have varied widely according to whether the advantages are seen to outweigh the disadvantages. In the United States where attitudes taken in different states have ranged from finding CLI to be in conflict with the state constitution, to accepting its introduction

without any form of blocking, the Federal Communications Commission has proposed that interstate CLI be made available with call blocking, the costs of CLI to be borne by the recipient of the call with the caller paying for blocking.

6.2 *EC Draft Directive on Telecommunications:* Article 12 would require call blocking and block blocking to be available 'via a simple technical facility', with line blocking being optional. The called subscriber must be able to prevent the identification of incoming calls on a case-by-case basis. Permanent suppression would be optional. All blocking by the caller would be able to be temporarily over-ridden by court order to prevent or pursue a criminal offence, and upon request of a subscriber to trace malicious calls, and permanently by emergency services and fire brigades.

6.3 *Council of Europe Draft Recommendation on Telecommunications:* This would require all subscribers to be informed of the introduction of CLI, and to be able to block CLI.

6.4 *International Conference of Data Protection Commissioners:* At the 1990 Conference a resolution was passed supporting free, simple, call blocking, which could be over-ridden for calls to the emergency services, and, in compliance with national law, to trace malicious callers. The resolution stated that the same principles should be adhered to for international calls.

7. CLI IN THE UNITED KINGDOM

7.1 As yet, CLI is not generally available in the United Kingdom. If operators were to facilitate its introduction it could be some time before it is in widespread use. Its adoption by private subscribers should be very gradual. As long as the facility remains an optional feature some people will choose not to purchase it. Thus the deterrent effect of CLI is likely to be almost immediate, as nuisance callers realise the increased risk of detection, but the privacy effects will depend on the rate of take-up of the facility.

7.2 Introduction of CLI in the United Kingdom should only be supported with safeguards. Call blocking with block blocking giving the caller the chance to remove the blocking and call again, would offer a compromise between the advantages and disadvantages of CLI. Line blocking should be offered as an alternative to call blocking. For call blocking to be used to this effect, however, it would need to be easy to use, and free to the subscriber. A system similar to that originally introduced in Canada, whereby blocking can only be put into effect by means of a call to the operator for which a charge is made, would be a disincentive to the use of blocking. The opposite system, where call blocking operates as the default system, would maximise privacy protection but reduce the advantages of CLI, except to the emergency services which could still override it. European proposals at various stages of development would not support this solution.

8. CONCLUSION

8.1 It seems likely that the systems operators will want to begin to introduce CLI generally within the next few years. Whereas, a few years ago, the Registrar could have taken the position that, given the introduction of CLI, call blocking should be the default system, the situation in many European countries and the provisions of the Council of Europe Telecommunications Recommendation and the Draft EC Directive on Telecommunications make this impractical. However, as argued in Section

5 above, the introduction of CLI would inevitably lead to breaches of the Data Protection Act unless it were accompanied by simple-to-use blocking facilities which were "free" to the user.

8.2 The Registrar therefore concludes that the introduction of CLI by a United Kingdom telecommunications operator would raise issues within his jurisdiction. Those issues can in his view only be addressed adequately by the introduction of other measures to ensure that the use of CLI does not contravene the Data Protection Principles. Those measures should include call blocking and line blocking. The system must not seek to discourage the use of the blocking facilities. It must, therefore, be simple to use and must not give rise to a direct charge to the subscriber who blocks CLI.

Appendix 3

Credit Reference and Third Party Information—The Enforcement Notice of the Data Protection Tribunal

The Enforcement Notice determined by the Data Protection Tribunal lies against the four main credit reference agencies. They are:

CCN Systems Limited
Consumer Affairs Dept.
PO Box 40
Nottingham NG7 2SS

Credit and Data Marketing Services Limited
CCA Dept
Dove Mill
Dean Church Lane
Bolton, Lancashire BL3 4ET

Equifax Europe Limited
Consumer Affairs Dept.
Spectrum House
1A North Avenue
Glasgow G81 2DR

Infolink Limited
CCA Department
38 Whitworth Street
Manchester M60 1QH

The enforcement notice reproduced here is for Equifax Europe Limited, but the notices for each of the other agencies are in exactly the same terms. (This presumes that the High Court accepts the consent order in respect of the appeals over the original CCN notice.)

IN THE DATA PROTECTION TRIBUNAL

BETWEEN:

EQUIFAX EUROPE LIMITED

Appellant

and

THE DATA PROTECTION REGISTRAR

Respondent

APPEAL DECISION—CONCLUSION

Members of the Tribunal: Aubrey L Diamond (Deputy Chairman), Alex Lawrence and Victor Ross.

1. On 28 June 1991 we issued the first part of our decision in this case, containing all our findings of fact and the reasons for the decision. We adjourned the hearing to a date when we could hear representations on the terms of the enforcement notice which we proposed to substitute under section 14(1) of the Data Protection Act 1984 for that served by the Data Protection Registrar on 29 August 1990. This document contains the concluding part of our decision.

2. The adjourned hearing was held on 12 February 1992. We heard submissions by counsel and solicitors as to the form of the enforcement notice, and also as to the date on which it should take effect. The Registrar's notice was to take effect on 31 July 1991, but in view of the time taken before the hearing of this appeal we thought at the first hearing that the revised form of enforcement notice should take effect on 1 January 1993. At the adjourned hearing on 12 February 1992 we were asked by Mr Chalton, representing the appellant, to reconsider that date, having regard to the time that it would take to make the necessary alterations to the appellant's programs, the date of the adjourned hearing and the delay after the first part of our decision before the appellant would have the definitive text of the enforcement notice. We have reconsidered the date, and think that in the interests of justice it is necessary to give more time than we envisaged last June. The enforcement notice set out below accordingly operates from 31 July 1993.

3. In the light of the parties' submissions we now conclude that the enforcement notice to implement our findings should issue in the following form:

   (1) That, subject to paragraph (2) below, from 31 July 1993 Equifax Europe Limited ("Equifax") shall cease to extract personal data relating to the financial status of individuals by any extraction program whereby (i) such personal data is extracted by reference to the current or previous address or addresses of the subject of the search ("the subject") and (ii) there is extracted, in addition to information about the subject, any financial information about any other individual who has been recorded as residing at any time at the same or similar, current or previous, address or addresses as the subject.

   (2) Subject to paragraph (3) below, nothing in this notice shall prevent the extraction of information about any other individual, recorded as residing at the same present or previous address as the subject concurrently with the subject, who—

      (a) (i) has the same surname, and forenames or initials where these are recorded, as the subject, or

(ii) has a name sufficiently similar to that of the subject for it to be reasonable to believe that he or she is the subject, or

(b) (i) has the same surname as the subject, or

(ii) has a surname sufficiently similar to that of the subject for it to be reasonable to believe that it is the same surname,

and where in either case it is reasonable to believe that he or she has been living as a member of the same family as the subject in a single household, or

(c) does not have the same surname as the subject but in respect of whom, on the basis of information obtained before extraction, it is reasonable to believe

(i) is the subject or

(ii) has been living as a member of the same family as the subject in a single household.

(3) In paragraph (2) above—

sub-paragraphs (a) and (c)(i) shall not apply where there is information in the possession of Equifax from which it is reasonable to believe that the individual is not the subject;

sub-paragraphs (b) and (c)(ii) shall not apply where there is information in the possession of Equifax from which it is reasonable to believe that there is no financial connection between the individual and the subject.

28 February 1992 Chairman

Appendix 4

The Agreement in the Enforcement Action against the Halifax Building Society

IN THE DATA PROTECTION TRIBUNAL

IN THE MATTER OF THE DATA PROTECTION ACT 1984 AND IN THE MATTER OF THE REGISTRAR'S ENFORCEMENT NOTICE TO HALIFAX BUILDING SOCIETY DATED THE 9TH DAY OF FEBRUARY 1989

In consideration of the withdrawal by the Registrar of the aforesaid Enforcement Notice against Halifax Building Society ("the Society") the Society undertakes and agrees as follows:

1. That in response to subject access requests made pursuant to section 21 of the Data Protection Act 1984 the Society shall henceforth make the same level of response as was made to (name of complainant) in the totality of the Society's responses in December 1987, August 1988, December 1988 and February 1989 (including in such response the data items of the type which were the subject of the Registrar's second preliminary notice against the Society dated the 12th June 1989 ("the Second Preliminary Notice")).

2. That the Society will also send to each data subject in response to a subject access request and at the same time as it makes the response referred to in paragraph 1 above a notice in the agreed form annexed hereto, marked Appendix 1.

3. That in any instance in which the data subject is genuinely disputing or querying any transaction or transactions the Society will (in addition to the response and notice referred to in paragraphs 1 and 2 above) disclose to the data subject the relevant details of such transaction or transactions sufficient to permit the data subject to identify the same and which will include at the least the date and time when the transaction was made at the ATM, the amounts involved, the nature of the transaction and the location of the ATM (including, where more than one ATM is situated at a relevant location, the identity of the ATM in question). The Society will disclose this information other than as part of their response under the Data Protection Act 1984 and will do so only from information which they may hold on the Journal Roll from the ATM in question. For the avoidance of doubt nothing in this agreement shall be construed as a restriction on or exclusion of the powers of the Registrar to take action against the Society in the event of any future breach of the Data Protection Act 1984.

4. That the Society concedes that the data the subject of the Second Preliminary Notice is

   (a) personal data within the meaning of the Data Protection Act 1984; and

   (b) not generally data to which the exemption in section 28 of the Data Protection Act 1984 would normally apply.

5. That the Society concedes for the purpose of this Appeal that the six categories of data the subject of this Enforcement Notice ("the six disputed categories") are personal data within the meaning of the Data Protection Act 1984 and that the Registrar shall be entitled to refer to and rely upon this concession in any future proceedings against the Society.

6. That both the Society and the Registrar reserve their positions in relation to the effect and the interpretation of section 28 of the Data Protection Act 1984 in any future proceedings against the Society.

7. That the Society agrees to withdraw this Appeal.

Signed: Robert S Smith QC and David Hatton, Counsel for the Society
Henry Carr, Counsel for the Registrar
Dated: Monday, 6 January 1992

Appendix 1

Halifax Building Society
Notice to Data Subjects

The Society is pleased to supply you, upon your request, with personal data which the Society holds about you. Please do not hesitate to contact the Society if you require any further assistance in relation to this.

In addition to the information enclosed, the Society would wish you to know that it has not included certain details concerning transactions on your account, such as the card number, the identification of the computer terminal at which a transaction is processed and the identity of the automated teller machine at the transaction location.

The Society, like all reputable financial organisations, is concerned to ensure the safety of its customers' funds. Our experience has shown that in order to protect the security and privacy of your account and those of other customers these details concerning transactions on accounts need to be kept confidential to only a small number of the Society's staff. Under Section 28 of the Data Protection Act 1984, the Society considers it is not obliged to disclose information which is likely to prejudice the prevention or detection of fraud or crime. This is one of the Society's reasons why these details have been omitted.

We stress that these details do *not* include details of your home, address, financial circumstances, the balance of your account or any views the Society or anybody have expressed about you. All of this has been made available to you. If it should transpire that there is a genuine need on your part to know all or part of the details concerning transactions on your account, the Society will always be pleased to consider your request for information and will do all it can to assist you.

Furthermore, if you are not satisfied with the response of the Society to your request, you are entitled to complain to the Data Protection Registrar at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.[1]

1. This is the new address of the Registrar, not that given in the original agreement.

Appendix 5

Research Results

In order to monitor attitudes and knowledge, amongst the public at large and amongst business establishments, research is undertaken from time to time. The work is carried out by professional research organisations under the direction of the Central Office of Information (COI). The COI analyses the results of the research and prepares tables and commentaries. Extracts from the tables and commentaries are reproduced in this Appendix. They fall into the two classes—those results relating to members of the public and those relating to business establishments.

(a) Members of the Public (Tables 1 to 9)

The research reported took place in February 1989, July 1990, March 1991 and March 1992. The research in 1990 took place at the close of a lightweight national television advertising campaign.

The research method was to conduct face to face interviews with a representative sample of the population selected by a mixture of random and quota methods. The sample size at each stage was around 1,000.

(b) Business Establishments (Tables 10 to 13)

The research reported took place in the first half of the years 1990, 1991 and 1992. The survey was conducted by telephone. There were 2,000 interviews with a representative sample of business establishments with fewer than 50 employees and 400 interviews with a representative sample of business establishments with 50 employees or more. The sample of business establishments was drawn from the business database of British Telecommunications PLC.

(c) Statistical Significance

"In the tables, * or ** denote a difference between two percentages which is statistically significant at the 95% level. The probability of a marked difference arising simply from sampling variation is 1 in 20 or less.

In calculating signficance a design factor of 1.4 has been applied in recognition of the clustered nature of the sample in which sampling error will have been greater than for a pure random sample of the population, in which each individual had an equal opportunity of being selected."

Table 1

Members of the public were asked to choose, from a list of issues, those which they considered to be very important.

	1989		1990		1991		1992
	%		%		%		%
Proportion saying the following are very important:							
Preventing crime on the streets	84		82		83	*	91
Improving standards of education	75		73	**	78	**	82
Protecting peoples rights to personal privacy	61		58	**	70	**	78
Unemployment	68		58	**	70	**	80
Inflation	61		56	**	62	**	66
Protecting freedom of speech	61		51	**	58	**	67
Making sure women have equal rights	52		49	**	54	**	61
Protecting the rights of minority groups	33		27	**	35	**	40

** = statistically significant over a two year period.
* = statistically significant over a one year period.

Comment:

For all the issues asked about, the number of people saying that they are "very concerned" has significantly increased over the last two years (except for preventing crime on the streets for which the significant increase was from 1991 to 1992).

Table 2

Members of the public were asked to name the five privacy issues which were of most concern to them. They were given a list of issues from which to choose.

	1989	1990	1991	1992
	%	%	%	%
Proportion saying the following are of most concern:				
Keeping personal information/ details private	76	72	74	76
Protecting the privacy of your own home/property	74	72	74	78
Being able to do what I want in my own home	63	59	63	64
People telling me what to do/ interfering with my life	57	55	57	58
Organisations building up files of information about me	54	54	51	52
Stopping unwanted mail/telephone calls/selling	52	56	56	51
Individuals prying into my business	49	49	52	52

Comment

There has been hardly any change in the privacy issues of most concern to people.

Table 3

Members of the public were asked to say how concerned they were about the amount of information that is kept about them by various organisations.

	1989	1990	1991	1992
	%	%	%	%
Very concerned	39	43	40	39
Quite concerned	33	28	32	34
Neither/Nor	9	8	8	8
Not very concerned	13	13	13	12
Not at all concerned	4	5	6	5

Comment:
No change in the level of concern over the years of this survey.

Table 4

Members of the public were given a list of different types of information and asked to indicate their level of concern about organisations keeping this information without their knowledge.

	1989	1990	1991	1992
	%	%	%	%
Proportion saying very or quite concerned:				
Your savings	77	76	74	77
How much you earn	74	74	67	72
Court judgements	68	66	64	67
Credit ratings	65	66	64	68
Your visitors	62	60	57	60
Medical history	60	59	61	61
Education and job history	45	40	44	43
What you buy	38	33	34	39
Membership of clubs	31	28	27	27
Your TV viewing	16	11	12	12
What papers you read	16	15	18	14
Your age	12	16	14	15

Comment
No change of note in the level of concern about the above information being kept by organisations without an individual's knowledge. Financial information remains the area which generates the most concern.

Table 5

Members of the public were asked to say how satisfied they were that various organisations can be trusted to keep and use information in a responsible way.

	1989		1990		1991		1992
	%		%		%		%
Doctors and the NHS							
Satisfied	90		88		91		92
Not satisfied	4		5		5		5
Banks and building societies							
Satisfied	83		80		83	*	78
Not satisfied	9		11		10		13
Employers							
Satisfied	72		71		75		74
Not satisfied	12		11		10		11
Police							
Satisfied	72		71		69		72
Not satisfied	18		14	*	20	*	15
Inland Revenue							
Satisfied	66	*	60	*	66		68
Not satisfied	19		19		19		17
Schools and colleges							
Satisfied	61		61		65		66
Not satisfied	15		11		12		12
DHSS							
Satisfied	59		58		61		63
Not satisfied	22		20		18		16
Shops and stores							
Satisfied	31		33		35		36
Not satisfied	43	*	32	*	39		41
Credit reference agencies							
Satisfied	27		26	*	31	*	25
Not satisfied	47		44		44		49
Mail order companies							
Satisfied	25		21		23		23
Not satisfied	55		49	**	53	**	57

** = statistically significant over a two year period.
* = statistically significant over a one year period.

Comments:

Some small but statistically significant changes from last year: fewer trust banks and building societies; the proportion trusting credit reference agencies has fallen back to the 1990 level; and, since 1990, there has been a gradual increase in dissatisfaction with mail order companies. On the other hand, the number who do not trust the police has dropped to the 1990 level.

Table 6

Members of the public were asked to say what importance they attached to various rights.

	1989		1990		1991	1992
	%		%		%	%
Proportion saying the following rights are very important:						
To correct errors in information about yourself	83		82		84	83
To know what the information about you is being used for	81		80		81	80
To be told who the information about you is being passed to	80		81		83	83
To be told where the information about you came from	79		78		78	77
To see what information is held about you	75		75		79	77
To have yourself removed from lists or files	79	*	64	*	75	78
To add things to the information about yourself	64		64		66	68

* = statistically significant over a one year period.

Comment:

No change from last year. These figures have remained very stable throughout the course of the research with the exception of the changing proportion between 1989 and 1991 who feel that the right to have yourself removed from files and lists is very important.

Table 7

Members of the public were asked questions to ascertain whether they were aware of the Data Protection Act, whether they had used the Act and how useful they considered the Act to be.

	1989	1990	1991	1992
	%	%	%	%
Aware that there is a law concerning rights about information kept on individuals	18	18	22	22
Spontaneous awareness of the Data Protection Act	6	9	8	9
Prompted awareness of the Data Protection Act:				
Definitely heard of	16	18	18	20
Think so	9	12	11	9
TOTAL AWARENESS OF THE DATA PROTECTION ACT	31	38	37	38
Made use of the Data Protection Act	2	2	3	3
Think the Data Protection Act is very useful	61	60	66	67
AWARENESS OF THE DATA PROTECTION REGISTRAR	23	35	36	34
TOTAL AWARENESS OF DATA PROTECTION*	42	53	53	51

*Anyone who has either definitely heard or thinks he or she has heard of the Data Protection Act and/or heard of the Data Protection Registrar.

Comment

There have been no changes this year in the levels of awareness of the Data Protection Act or of the Data Protection Registrar.

Awareness is higher among: males (55%); 35-44 year olds (68%); and amongst the AB (middle to senior management) (73%) and C1 (clerical and lower management) (71%) socio-economic groupings.

Table 8

Without prompting, members of the public were asked to say what they knew about the Data Protection Act.

	1989	1990	1991		1992
Base: all aware of the Data Protection Act	%	%	%		%
Right to find out what information is held about you	22	18	26	*	16
Protecting your rights about what information is kept on you	12	17	13	*	21
Firms need to register	5	8	7		6
Have to pay	5	3	2		1
Able to correct wrong information	3	10	11		7
Only see computer records	3	1	2		2

* = statistically significant over a one year period.

Comment

In 1992 there has been a fall in the proportion mentioning the right to find out what information is held about you and an increase in mentions of protecting your rights about what information can be kept on you.

Table 9

Members of the public were asked to indicate which functions they thought the Data Protection Act performed.

	1989	1990		1991		1992
Base: all aware of the Data Protection Act	%	%		%		%
Proportion saying the Data Protection Act performs the following functions:						
Enforcing your right to see information kept about you	56	61		64		63
Enforcing your right to correct information kept about you	55	59		65		62
Controlling information that can be kept on you	48	50		53		56
Monitoring all personal information on paper as well as on computer	35	32		33		35
Stopping organisations passing information about you to others	34	33	**	35	**	43
Making people who misuse information liable to imprisonment	38	28	**	35	**	40
Providing compensation if you are harmed by the misuse of information	28	23		24		29

** = statistically significant over a two year period.

Comment

Compared with 1990, significantly more people believe the Data Protection Act stops organisations passing on personal information to others and that the Act makes people who misuse information liable to imprisonment. Both of these are misconceptions.

Table 10

Businesses were asked about their use of computers.

	Small Companies (Fewer than 50 employees)			Large Companies (50+ employees)		
	1990	1991	1992	1990	1991	1992
Sample size:	1999	2001	2047	398	396	402
	%	%	%	%	%	%
Type of computer:						
Personal/micro	24	27 *	35	77	89	89
Multi-user or mini computer	7	9	10	58	71	73
Word processor	14	20	19	69	81	70
Computer access terminal	6	8	7	44	49	45
Mainframe	1	5	4	42	36	35
Data processing carried out by outside body	5	6	4	19	25	28
TOTAL with computers or using computer bureau	40	45 *	50	98	100	100

* = statistically significant over a one year period.

Comment

Use of computers amongst small companies continues to increase and has now reached one in two.

Table 11

Those businesses which used computers were asked whether they held personal records on them.

	Small Companies (Fewer than 50 employees)			Large Companies (50+ employees)		
	1990	1991	1992	1990	1991	1992
Base: all using computers:	840	1036	1134	391	393	402
	%	%	%	%	%	%
Hold personal records on computer						
Yes	33	43	46	74	97	100
No	58	52	50	19	—	—
Don't know	9	4	4	6	3	—

Comment

Just under half of all small companies that use computers (just under a quarter of all small companies) hold personal records on them. All larger companies have computers and keep personal records on them.

Table 12

Those businesses which hold personal records on computer were asked about their awareness of the Data Protection Act and the Data Protection Registrar.

	Small Companies (Fewer than 50 employees)			Large Companies (50+ employees)		
	1990	1991	1992	1990	1991	1992
Base: all who hold personal records:	362	520	533	318	383	402
	%	%	%	%	%	%
Prompted awareness of the Data Protection Act	70	87	88	95	95	97
Semi-prompted awareness of the Data Protection Registrar*	44	47	* 58	67	61	* 72

* = Statistically significant over a one year period.

Comment

Awareness of the Data Protection Act is lower in small manufacturing companies (21% not aware) than in small service companies (8% not aware).

Awareness of the Data Protection Registrar was significantly higher than last year amongst respondents from both small and large companies. Among the large companies, awareness of the Registrar was directly related to size of company, eg. 50-99 employees 65% aware, 500+ employees 85% aware.

*Respondents were asked to select from a list of likely sounding titles the person responsible for looking after the public's interest with regard to personal records held on computer.

Table 13

All businesses holding personal records on computer were asked questions to ascertain their awareness of the need to register under the Data Protection Act and that the Act imposes other obligations (for example compliance with the Data Protection Principles).

	Small Companies Fewer than 50 employees)			Large Companies (50+ employees)		
	1990	1991	1992	1990	1991	1992
Base: all with personal records on computer:	362	520	533	318	383	402
	%	%	%	%	%	%
Aware of the need to register	51	62	62	85	82	85
Awareness of other obligations (as well as the need to register)	26	26	29	47	44	45

Comment:

No change from last year in either awareness of the need to register or in awareness of other obligations placed on organisations holding computer records on individuals.

Awareness of the need to register is connected with size. Over the last three years awareness has been consistently lower in both the large and the small establishment samples among the smallest size categories (1-2 employees and 50-199 employees respectively).

Awareness has also been consistently lower over the last three stages of research among respondents from the distribution sector in both the large and the small establishment samples.

Appendix 6

Unaudited Financial Statement
For the Year Ended 31 March 1992

STATEMENT OF RECEIPTS AND PAYMENTS FOR THE PERIOD 1 APRIL 1991 TO 31 MARCH 1992

	Notes	*1991/92*		*1990/91*	
		£	£	£	£
H.M. Grants received	2	3,423,094		3,152,796	
Operating receipts	3	2,254,965	5,678,059	1,944,366	5,097,162
Salaries and Wages		1,351,156		1,166,112	
Other operating payments	4	1,957,527	3,308,683	1,935,211	3,101,323
Surplus from operations			2,369,376		1,995,839
Other Receipts	5	169,749		123,929	
Other Payments	5	92,630	77,119	51,427	72,502
Surplus for Year			2,446,495		2,068,341
Appropriations	6		2,446,915		2,093,430
Excess of receipts over payments for the period			(420)		(25,089)

STATEMENT OF BALANCES AS AT 31 MARCH 1992

	Note	*1992*	*1991*
		£	£
Balance at beginning of period		24,230	49,319
Add excess of receipts over payments for the period		(420)	(25,089)
	7	23,810	24,230

The following Notes form part of this Statement.

Notes to the Statement

		1991/92 £	1990/91 £
1.	These accounts are drawn up in a form directed by the Secretary of State, and approved by the Treasury.		
2.	HMG Grants Received.		
	Grants received from Class IV Vote 3 Subhead I6 1991-92	3,423,094	3,152,796
3.	Operating Receipts		
	Receipts from registration fees	2,254,965	1,944,366
4.	Other Operating Payments		
	Rents & rates	257,565	224,601
	Maintenance, cleaning, heating & lighting	130,532	54,496
	Office supplies, printing, stationery	63,830	54,875
	Postage & telephones	70,240	53,460
	Travel & subsistence	114,644	113,051
	Staff recruitment	8,447	11,759
	Specialist assistance	4,735	31,229
	Public relations	503,252	493,958
	Legal costs	64,763	67,439
	Staff training/health & safety	37,908	28,186
	Computer bureau	465,611	588,551
	Vehicle expenses	1,834	1,571
	Audit fee	5,730	5,100
	VAT	228,436	206,935
		1,957,527	1,935,211
5.	Other Receipts/Payments		
	Receipts		
	Pension contributions/transfers	77,400	12,609
	Bank interest	85,374	107,396
	Other interest	47	
	Speakers' fees	850	375
	Sale of Motor Van	2,750	
	Legal Costs recovered	3,328	3,549
		169,749	123,929
Payments			
	Purchase of computer hardware/software	53,987	22,460
	Purchase of furniture & other office equipment	17,746	22,302
	Purchase of Van	7,319	
	VAT	13,578	6,665
		92,630	51,427
6.	Appropriations		
	Amounts surrendered to the Consolidated Fund via the Home Office during the period		
	Registration fees	2,276,902	1,969,765
	Other	170,013	123,665
		2,446,915	2,093,430
7.	Balance at Period End		
	Cash at bank	23,433	23,950
	Cash held at offices	377	280
		23,810	24,230
8.	The Data Protection Registrar operates a non-contributory pension scheme to provide retirement and related benefits to all eligible employees. Retirement benefits are based on individual final emoluments. The scheme is funded on a pay-as-you-go-basis from Grant-in-Aid.		

Printed in the United Kingdom for HMSO
Dd 0507893, 7/92 C15 3383/3C O/N 202698 12310

HMSO publications are available from:

HMSO Publications Centre
(Mail, fax and telephone orders only)
PO Box 276, London SW8 5DT
Telephone orders 071-873 9090
General enquiries 071-873 0011
(queuing system in operation for both numbers)
Fax orders 071-873 8200

HMSO Bookshops
49 High Holborn, London, WC1V 6HB
071-873 0011 Fax 071-873 8200 (counter service only)
258 Broad Street, Birmingham, B1 2HE
021-643 3740 Fax 021-643 6510
Southey House, 33 Wine Street, Bristol, BS1 2BQ
0272 264306 Fax 0272 294515
9-21 Princess Street, Manchester, M60 8AS
061-834 7201 Fax 061-833 0634
16 Arthur Street, Belfast, BT1 4GD
0232 238451 Fax 0232 235401
71 Lothian Road, Edinburgh EH3 9AZ
031-228 4181 Fax 031-229 2734

HMSO's Accredited Agents
(see Yellow Pages)

and through good booksellers

ISBN 0-10-206493-8

9 780102 064933