SEVENTH REPORT of the Data Protection Registrar June 1991

THE DATA PROTECTION REGISTRAR

LONDON : HMSO

SEVENTH REPORT

of the

Data Protection Registrar

June 1991

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

Ordered by the House of Commons *to be printed 16 July 1991*

LONDON: HMSO

£11.40 net

553

Contents

1 Introduction

This Report is for the year ending 31 May 1991. It follows a similar format to previous Annual Reports with the various sections broadly equating to the activities of the Office. However, this year the Report also includes sections on the European Commission's Draft Directive on Data Protection and on the first appeal hearings by the Data Protection Tribunal.

During the year, significant changes have been made in the way the Office is staffed. Whilst these changes have taken place, the complexity of work coming into the Office has generally continued to increase. It is a tribute to the loyalty and dedication of staff that they have taken all this in their stride. I should again like to express my appreciation for their unswerving support.

2 Some Significant Issues

In this section I deal with a number of significant issues with which my Office is currently concerned.

There was a helpful opportunity to exchange views on some of these issues when I gave evidence to the Home Affairs Committee of the House of Commons in October 1990. The discussion at that meeting concentrated in particular on matters raised in my last Annual Report. The Committee published its conclusions in December 1990 in its First Report of the 1990-91 Session. I am grateful for the support which the Committee expressed for the work of my Office. I also appreciate the similar support given in the Government's response to the Committee's recommendations.

The Home Affairs Committee recognised that a wide range of legislation has implications for data protection. It stressed the importance of government departments contacting my Office at an early stage in the formulation of new legislation, so that advice can be given on relevant data protection issues. At about the same time, Ministers, following a series of Parliamentary Questions, had also reminded departmental staff of this need.

I have followed up by approaching the Permanent Secretaries of all relevant departments to try to establish more formal and on-going liaison arrangements. I received a positive response to these approaches and my Assistant Registrar who deals with the government sector has taken matters forward with more detailed meetings. There is now evidence that more government departments are seeking advice from my Office as a matter of course. I appreciate that government departments are complex, often large organisations and it will be necessary to monitor the effectiveness of these newly established liaison arrangements.

Some of the matters which the Home Affairs Committee considered are referred to in this section. Others, including the European Commission's Draft Directive on Data Protection, knowledge of the Act amongst the general public and the financing of the Office, are dealt with in separate sections.

(a) The Health Service

Developments in the health sector are leading to a much greater use of information technology both in the management of the health service and in the provision of clinical care.

The introduction of an internal market in the National Health Service (NHS) involves contracts for the provision of health care and requires a flow of patient information between "providers" and "purchasers". Patient information is also being collected by District Health Authorities to assess the health status and needs of the local population. Both of these demands are being met through the circulation within the NHS of what is called a "contract minimum data set".

Information about individuals' health is very sensitive and my staff are investigating the content and use of these "data sets" so as to determine that these comply with the requirements of the Data Protection Principles. The confidentiality of such sensitive information is of particular concern. Questions arise as to who will have access to health information; and whether those who

are concerned with administration rather than clinical care will be able to identify individuals and all their health details.

In parallel with the development of the "contract minimum data set", NHS numbers, which are unique to each member of the population, will be increasingly used to identify patients. Consideration is being given by the Department of Health to re-issuing unique numbers to a common format in order to facilitate their use. Care will be needed to hold the use of this number within the NHS.

The Interprofessional Working Group set up by the British Medical Association (BMA) has produced a draft Code of Confidentiality of Personal Health Information. I would welcome the adoption of this Code which sets strong constraints on the use and disclosure of such information. The Code could form the basis of an order to supplement the Data Protection Principles under Section 2(3) of the Data Protection Act, which would provide an enforceable standard underpinning the confidentiality of health data.

I understand that the Department of Health has not supported a statutory strengthening of the Data Protection Principles in respect of medical confidentiality. The Department is now working on draft non-statutory guidance and I have been assured I will be consulted as to the data protection implications. The Scottish Home and Health Department has issued its own non-statutory Code of Practice on the Confidentiality of Personal Health Information. I was not consulted on the data protection implications of this Code. I believe further consideration needs to be given to the circumstances in which the Code assumes that individuals have given implied consent to particular uses of personal health information, for example, for medical research. A Council of Europe Working Party is also considering appropriate safeguards for personal health information and I await its conclusions with interest.

The increasing use of computers in the health service has given added significance to the importance of ensuring information is fairly obtained from patients. This is required by the First Data Protection Principle. My staff are in discussion with officials of the Scottish Health Service which I hope will lead to the issue of appropriate guidance to hospitals in Scotland. The matter has also been raised with the Department of Health.

The NHS Management Executive has published an evaluation report on the "Care Card" trial. This was an experimental project carried out in the Exmouth area. In the trial, patients were issued with smart cards (essentially small computers on plastic cards) which contained their medical records. The information on the card was accessible to medical staff or pharmacists and new information could be added by them. The Department of Health is now considering further trials to assess the benefits of using patient data cards and/or other technologies, such as networking, to transfer patient health information between health care professionals.

My staff maintained contact with the original trial and will do the same with future trials. The current evaluation report has not indicated any major data protection problems, but more evaluation work is needed. It is interesting to note that the European Commission is attempting to formulate a Community strategy on patient data cards through its Advanced Informatics in Medicine (AIM) project and I am staying in touch with this development.

Finally, I am pleased to have been associated with the General Medical Services Committee of the BMA in the production of a Data Protection Code of Practice for General Practitioners.

(b) Policing and Criminal Justice

There are fifty-two main police forces within the United Kingdom. In addition, there are a further seventeen policing bodies ranging from the British Transport

Police to the Royal Parks Constabulary. Within the police service there are certain common policing activities such as Regional Crime Squads and common police services such as the Police National Computer and the National Identification Bureau. The Home Office, whilst not having an active policing role, is involved in matters of policing policy and the provision of common services such as the Police National Computer.

Although policing is primarily a local matter, there has been an increasing trend towards nationally coordinated activities, particularly in matters of serious crime or where there is an international dimension. Thus, there has been the establishment of the National Drugs Intelligence Unit and the National Football Intelligence Unit and a recent appointment of a Head of a National Criminal Intelligence Service.

At policy level, the key link between my Office and the police sector is through the Association of Chief Police Officers (ACPO) Working Group on Data Protection. This Working Group includes representatives of a variety of forces and of ACPO Scotland. ACPO's fundamental coordinating and information dissemination role is being supplemented by individual police forces, which have established direct contacts with my Office for more detailed consideration of matters of particular concern to them. Additionally my staff are being increasingly invited to attend regular Regional Data Protection Conferences at which matters of mutual interest are discussed. I am pleased to see these widening contacts and will be looking to extend them in the future to less well known policing bodies such as Port Police Forces.

Whilst the police are a key element in the criminal justice system they are not the only one. Other bodies with which my Office has established contact include: the Lord Chancellor's Department (Crown Courts); the Home Office (Magistrates Courts); the Probation Service; the Crown Prosecution Service; the Crown Office and Procurator Fiscal Service in Scotland; and the Northern Ireland Courts Administration.

There are increasing moves to coordinate computer developments within the criminal justice system. A Home Office led committee for the Coordination of Computerisation in the Criminal Justice System (CCCJS) has been established to promote the sharing of information. Through contacts with this committee and with other organisations in the criminal justice system my staff are seeking to give guidance on the data protection aspects of these new computing developments.

(i) *Criminal Records*

Criminal records are of interest not only to the police, but also to others in the criminal justice system such as the courts and prosecuting authorities. At present, records about individuals who commit reportable offences are maintained centrally on microfiche by the National Identification Bureau which is managed by the Metropolitan Police. These records contain policing information as well as a factual account of an individual's criminal history. An index to all records is maintained on the Police National Computer.

In last year's Report, I referred to concerns expressed by the Home Affairs Committee of the House of Commons about the current National Criminal Records System. The Committee made recommendations about the scope, nature and availability of these records as well as about the methods of collecting and maintaining them.

The Home Office responded to those concerns by establishing a scrutiny of the National Criminal Records System. Many data protection issues arise from the holding of potentially sensitive personal information such as criminal records. These issues include: who should be the record keeper; the extent

of the records; who should provide information for the records; who should be entitled to see the records; and for how long the records should be retained. I was pleased to be invited to provide written comments and to meet with the scrutiny team. I have expressed support for a publicly accountable National Criminal Records Agency and a system of statutorily regulated disclosures. I am particularly concerned to see safeguards for individuals and an end to the current and increasing practice of individuals being forced, by employers and others, to use their own subject access rights to open up access to these records.

The scrutiny team has now reported to Ministers and I look forward to seeing its conclusions which I understand are to be published.

(ii) *The New Police National Computer System*

Many of the developments towards integration within the criminal justice system and reorganisation of criminal record keeping will focus on the Police National Computer (PNC). The migration of certain existing applications to the new Police National Computer (PNC2) is due to take place shortly. Proposals for further developments such as an integrated criminal intelligence system and the national criminal records system mentioned above, allied with the increased computer power and flexibility provided by PNC2, demand careful attention to data protection requirements.

Supporting technological developments such as photographic image storage systems, automatic fingerprint recognition and electronically searchable voice and video tapes will also raise novel and difficult problems.

(iii) *Cooperation in International Policing*

The arrangements surrounding the operation of the Channel Tunnel will require British Police, Customs and Immigration officials to operate in France; and French Police and Government officials to operate on trains in the United Kingdom and in the Tunnel terminal control zone in Kent.

My staff have opened discussions with the police, Government departments and the French data protection authority over the data protection implications of these arrangements. A particular issue concerns whether, or how, United Kingdom and French laws are to apply to activities in the two countries.

In a wider context, the effective removal of border controls between states and the cross-border activities of criminals is requiring increased cooperation between police forces of different countries. Already the Schengen Agreement, removing border controls between France, Germany and the Benelux countries, has led to the proposed Schengen Information System, a common database to aid policing cooperation. Similarly Interpol has recently established an improved computer facility and the TREVI group, another co-operative European venture, is also considering a common police information system. I am seeking information on all these developments so that I can give consideration to ways in which the requirements of the Data Protection Act are met.

(iv) *DNA Profile Databases*

The technique of producing a "unique" personal DNA profile from genetic material is becoming an increasingly common forensic tool which is used to aid detection where genetic material is left at the scene of a crime. There is the potential for an individual's DNA profile to be recorded in a similar manner to his or her fingerprints. The Home Affairs Committee has suggested that a DNA profile database on the whole male population would provide

considerable benefits for the police. The Commissioner for the Metropolitan Police has also put forward the idea of "a comprehensive index of DNA profiles" for public debate.

The Home Secretary, in responding to the Home Affairs Committee has indicated that the Home Office is considering a number of important legal and ethical questions relating to the establishment of a DNA database. Consideration will be given to the Committee's support for the creation of a database on the whole male population as well as other proposals. The Government has also confirmed that the Forensic Science Service and the National Identification Bureau are examining the possibility of including DNA profiles in criminal records.

I have had an initial discussion on DNA profiles with the Director of the Metropolitan Police Forensic Science Laboratory and will approach other interested parties, such as the Home Office Forensic Science Service and the Scottish Forensic Science Service. I shall also wish to take note of work currently being carried out in the Council of Europe on DNA profiling for forensic purposes.

Establishing a database of DNA profiles calls for careful consideration of data protection requirements. Issues such as obtaining, disclosure, relevance, accuracy, retention and security of such sensitive data will all be important. These issues will arise in connection with DNA profiles held to supplement criminal records. They arise starkly if the database is one of the population at large, regardless of any specific supporting justification.

(c) The Child Support Bill

The Child Support Bill, which makes provision for the assessment, collection and enforcement of payments for child maintenance, was referred to me at an earlier stage than previously has been the practice with new legislation. I welcome this.

The Child Support Agency and the Child Support Officers, which the Bill envisages, will have wide ranging powers to gather information. These powers will be exercised under regulations made by the Secretary of State. Information obtained under such regulations will not be subject to the "fair obtaining" requirement of the First Data Protection Principle. The purpose for which information is required may, of course, be obvious from the circumstances in which it is obtained, but there will be no statutory requirement to make matters clear.

The Fourth Data Protection Principle states that personal data should be "adequate, relevant and not excessive". In the light of this, I have recommended that consideration is given to ensuring that the powers to collect information should apply only to information expressly specified in the Act or Regulations. Whilst obviously this approach will not, by itself, ensure that this Principle is complied with, it is more likely to encourage compliance than an approach which gives the Agency and Support Officers more sweeping general powers.

I also drew attention to the Sixth Data Protection Principle which states that personal data "shall not be kept for longer than is necessary". In order to comply with this Principle, procedures need to be established to ensure that personal data are deleted promptly as soon as they cease to be relevant for establishing maintenance contributions in respect of a particular child or children.

On the face of it the Third Data Protection Principle requires that personal data should not be used or disclosed in any manner incompatible with the purposes for which they are held. In practice this is not so, as the interpretation of this

Principle deems uses and disclosures to be compatible—however unlikely or unreasonable—provided that they have been registered. In view of this I have asked the Department of Social Security to consider reaffirming commitment to the Third Data Protection Principle by confining the use and disclosure of personal data to purposes wholly consistent with the reason those data are held, namely the efficient administration of the assessment and collection of child maintenance.

Once the Bill has passed through Parliament, I shall take these points up again with the Department of Social Security as matters for resolution through regulations and operating procedures.

(d) Uses of the Electoral Register

Last year I referred to new regulations issued by the Home Office which constrained Electoral Registration Officers (EROs) to supply copies of their registers to anybody on demand. I explained that the Home Office Minister had supported, in principle, my suggestion that EROs should publish a list of those who had bought their registers. This would enable individuals to trace who had purchased information about them and use their rights under the Data Protection Act to check on the subsequent holding and use of their details.

During the year, I have consulted the local authority associations (in particular, The Association of District Councils (ADC), the London Boroughs Association (LBA), the Association of Metropolitan Authorities (AMA), the Association of London Authorities (ALA) and the Convention of Scottish Local Authorities (COSLA)) and have been pleased to receive their support. The Home Office has also carried out separate consultations with other local authority representatives and received similar support.

Whilst the Home Secretary does not have power to require EROs to publish information on purchasers, I am pleased that a scheme is being prepared by the Home Office which encourages this. I am awaiting details of the scheme from the Minister.

(e) Computing in Schools

The rapidly growing use of computers in schools and changes in education legislation have focussed attention on the application of the Data Protection Act in local education authority (LEA) maintained schools. The Department of Education and Science (DES) consulted me on draft guidance to LEAs and LEA maintained schools which identified School Governing Bodies, as well as LEAs, as possible data users for personal data held in schools. Legal advisers from my Office and the DES met and identified that, in addition, a Headteacher might be a data user if certain categories of personal data were held. The possibility of the LEA, the Governing Body and the Headteacher all being data users in their own right in any one school arises from the distinct statutory responsibilities of each. This leaves them each independently exercising control over the content and use of personal data held in connection with those responsibilities.

My staff have assisted officials of the DES in redrafting their guidance to clarify the registration requirements for personal data held in schools. There will inevitably be a substantial number of Governing Bodies and Headteachers who will be required to register. I am aware that it will take some time for LEAs and schools to determine whether and how the Act applies, but anticipate that it should be possible to organise any necessary registrations by the end of this calendar year. I am also conscious of the financial burden that will be placed on LEAs and individual schools by registration fees and have asked the DES whether it would be possible for the cost of fees to be met from central funds. I understand

that the DES will give consideration to additional funding for these fees in future years if not in this year.

(f) The Community Charge

In my last report I expressed disappointment at the problems which had arisen with a large number of Community Charge Registration Officers (CCROs) in connection with the initial compilation of their community charge registers. This year my staff have renewed their efforts to ensure that similar difficulties are not encountered as CCROs strive to maintain and update their registers. Thus far, CCROs' 'rolling canvass' forms have not caused many problems and although further complaints have been received about forms seeking details of changes in individuals' circumstances, I am hopeful that these can be resolved without it being necessary to proceed with further formal enforcement action.

Looking to the future, the community charge is to be replaced by a new system of finance for local government and I have received assurances from the Department of the Environment that, as and when details become clear, I will be fully consulted as to the data protection implications of the new system. I have already commented on draft clauses in a Bill dealing, amongst other things, with the valuation of all domestic properties in England and Wales.

(g) Profiling of Individuals for Direct Marketing

The direct marketing industry is increasingly building larger and more detailed databases of information about individuals. These are often used to form profiles of individuals in order to target them for mail about particular products and services. In so far as this results in individuals receiving information in which they are interested and not irrelevant mail, then it can avoid the annoyances which unsolicited marketing literature can cause; but the position is not as clear or straightforward as this.

Over the last six months, my staff have been undertaking some research into profiling techniques and the targetting of direct mail. The objective is to get a sound understanding of the practices of the direct marketing industry before considering the position in respect of data protection requirements. The industry has been very helpful in providing information and joined in a day's exchange of views in May 1991. This particular meeting was also attended by a number of representatives of data protection authorities in Europe.

The issues under consideration include: the collection of information via life style questionnaires; the relationship of census or geographically based data to individuals; the use of publicly available information such as electoral and share registers; the range of information held on individuals; and the ascription of information to individuals.

My staff will be holding further discussions with the industry on these issues. Initially, attention will be directed to lifestyle questionnaires and the content and clarity of notification given to individuals who are asked to complete them, as to why the information is wanted. The question of assembling information on an individual from a variety of sources will be considered in a wider study of data matching.

(h) The Finance Sector

(i) *Banking Services*

The Review Committee on Banking Services Law (the "Jack Committee") reported 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 responded to the Committee's report through "Banking Services: Law and Practice," a White Paper published in March 1990. The Government's conclusions were also supportive of data protection objectives concluding, for example, that an individual should be able to opt out of the use of his or her banking information for marketing or credit reference purposes except, in the latter case, where "black" information (information about defaults) is concerned. The Government wished to see its conclusions introduced through a code of practice for banks and building societies.

A Working Group comprising representatives of the Association for Payment Clearing Services, the British Bankers Association and the Building Societies Association was set up in March 1990 to produce a non-statutory Code of Banking Practice. The purpose of the Code is to set out standards of banking practice to be observed by banks, building societies and card issuers when dealing with their personal customers in the United Kingdom.

The Working Group sought my comments on the draft of the Code and arranged a meeting to consider these. There was a very open and helpful discussion at this meeting. I expressed a concern that the draft Code appeared to reduce the level of protection given to individuals by the present banker's duty of confidentiality. I also took the view that the draft Code did not meet the level of protection envisaged in the Government's White Paper in respect of the use of customers' information for purposes other than administering an account, for example, use for direct marketing.

I understand that the Working Group is reconsidering the draft Code and may be making some modifications. Another meeting is being arranged to consider this second version of the Code.

(ii) *Financial Intermediaries*

I have received a number of complaints from members of the public concerning questionnaires used by financial intermediaries selling investment products covered by the Financial Services Act 1986 (FSA). The questionnaires asked for detailed information about a client's financial and personal circumstances with the purpose of satisfying the 'know your customer' rules made under the FSA and to ensure that 'best advice' is given. The complainants felt these questionnaires were intrusive and were concerned as to how the details would be used or disclosed.

As it appeared that a significant number of intermediaries intended to hold some or all of this information on computer, I felt it would be helpful to these data users to provide guidance on how to comply with the 'fair obtaining' requirement in the First Data Protection Principle whilst meeting their obligations under the FSA. Guidance Note 24, covering these matters, was published by my Office in the Spring of this year. This was promoted through a news release and by direct distribution of the Guidance Note to relevant trade associations, self-regulatory organisations and recognised professional bodies.

(iii) *Credit Reference*

Efforts here have been taken up with enforcement action in respect of the extraction of third party information by the main credit reference agencies. Information on this is given in Sections 4 and 6.

(i) Small Businesses

Research carried out by the Office in 1990 revealed a lowering level of awareness of the need to register amongst small businesses which hold personal data. This despite the fact that there was evidence of an increasing use of computers by such businesses. The position has improved somewhat in 1991, possibly because of the measures already put in train to alert small businesses and give them more information and advice.

The problem has been discussed with trade associations and other bodies representing small businesses. Arising from these discussions a number of pro-active approaches to raise awareness and compliance have been identified. Some approaches—such as the development of a range of simplified literature specially aimed at small businesses—are already being implemented. I am now reviewing a range of activities which may be helpful.

(j) Photographs on Driving Licences

The Driver and Vehicle Licencing Agency (DVLA) has circulated a consultation document on the proposal to introduce photographs on driving licences in Great Britain. At first glance this seems a fairly simple issue of improving matters in connection with driving laws. I understand that there is no intention to make the driving licence a de facto national identity card. Also, the Minister has made clear that there is no intention to change the rules to make drivers carry their licences at all times.

However, I do have some concerns about the practical effect of adding a photograph to a document held by over thirty million people. It seems inevitable that this will increase the attractiveness of the driving licence as a proof of identity in many ordinary everyday situations, such as opening a bank or building society account, hiring garden equipment or videos. There is clearly a danger that what starts as the preferred means of establishing identity in a variety of circumstances will in practice gradually become a de facto national requirement.

Moreover, the driver licence number is but a thinly disguised amalgamation of driver's initials and date of birth. Leaving aside the information which the number contains, its collection when the licence is produced as a means of identification raises the possibility that it will come to form a de facto national identifier.

It is claimed that the introduction of photographs on driving licences would make law enforcement easier. At the moment the police have no means of direct on-line access to driving licence records although the Government has announced plans to make available all driver details to the police in 1992. It is not clear if such details will be available on the new Police National Computer System (PNC2). If they are and the details included digitised photographs this could provide a significant new policing tool particularly if there were to be a trend to mobile data terminals. This may give rise to wider considerations of public policy.

It is for Ministers and Parliament to decide public policy in respect of the nature and use of driver information. It would be helpful if any introduction of photographs on driving licences were to be accompanied by a fresh consideration of such matters as controls on the obtaining, disclosure and use of driver information and on the occasions on which production of a driver's licence could be demanded.

(k) Uses of the National Insurance Number

Last year I expressed my concern about the possibility of the National Insurance Number creeping into wider and wider use to the extent that it became a de facto

national identity number. The Department of Social Security (DSS) has since confirmed that, though there is no specific statutory restriction, the Department's policy is to seek to restrict the use of this number to tax and benefit related purposes. This is a helpful policy, but without supporting statutory regulations, not necessarily perfect.

The policy itself already leads to the potential leakage of the National Insurance Number into private sector uses. For example, those providing Personal Equity Plans (PEPs) must collect the number so that plans can be validated with the Inland Revenue. Similar requirements have been introduced with regard to the Tax Exempt Special Savings Account (TESSA) scheme. I am pleased that, following representations from the DSS, the Inland Revenue have included in the TESSA Operator's Handbook a clear statement that the National Insurance Number should not be used for any other purpose than validating applications with them. A similar statement will appear in the PEP Operator's Handbook which is currently being revised.

A second problem arises from the framing of the Data Protection Act. When information is obtained under statutory authority it is always treated as having been fairly obtained. Therefore, because individuals are required to provide their National Insurance Numbers when making an application to a PEP or TESSA provider, that organisation is under no obligation to give any explanation for the use of that number. As it is by no means universally known by the public at large that the National Insurance Number is now effectively also an individual's tax reference number, this has led to complaints to my Office that could easily have been avoided if a simple explanation had been provided. Some PEP and TESSA operators do now provide an explanation.

Finally, there is the question of what sort of information falls under the statutory requirement. Care needs to be taken to limit this to what is strictly necessary. Under the TESSA requirements, for example, plan providers must collect both the National Insurance Number and date of birth of all applicants. Yet, the National Insurance Number itself is a sufficient identifier without date of birth. Nor is date of birth required to signify age, because individuals have to sign a statement that they are over eighteen. If the individual cannot provide his or her National Insurance Number, then date of birth may be necessary, but otherwise there seems no reason to collect and hold it. Unfortunately, the regulations governing this matter were made before my Office had chance to comment. I have asked the Inland Revenue to bear this point in mind for any further changes in the regulations.

(l) Telecommunications

The modernisation of telecommunications networks through such as digital exchanges, digitised transmission, and the Integrated Services Digital Network (ISDN), brings with it new data protection concerns. Modern networks have the potential to collect detailed information on the subscriber's use of the telephone system (numbers called, duration of call, time of day). The technology also facilitates the introduction of new facilities which themselves bring privacy concerns. Examples are itemised billing, and calling line identification.

Itemised billing, in which a statement of individual calls made from the subscriber's line is made available with the bill, is not new. However, it does call into question the appropriate balance between the privacy of the caller (where the caller is not the subscriber) and the called party and the legitimate interests of the subscriber in knowing what it is he is paying for. For example, there is the problem of protecting a member of a household who wishes to make calls to a counselling or help agency, details of which appear on the itemised bill. There seems no easy solution to this problem. I recognise the concerns which Data Commissioners in some other countries have expressed about itemised bills.

However, I do feel it is necessary to seek a solution which preserves the gain for customers in having itemised bills.

Similarly, the calling line identification facility, by which the number of a calling party is displayed on the receiver of the called party before the call is taken, raises privacy issues. At first sight, this appears to be a valuable facility which would help a subscriber to avoid taking unwanted or nuisance calls. On the other hand, a subscriber calling a commercial company or service may not wish his number to be announced beforehand in case he decides not to enter into any transaction with that company. The technology can provide safeguards for both the calling and the called party, for example, by allowing choices as to whether to use this identification facility or not. It seems appropriate that these safeguards should be built into the services offered.

These and other related issues in the telecommunications sector have been the subject of much discussion at international level. The discussion has been intensified by a European Commission initiative to introduce a draft directive concerning the protection of personal data and privacy in the context of telecommunications networks. The Council of Europe is also active having, through one of its working groups, produced a draft recommendation on this subject. The International Conference of Data Protection Commissioners also has a relevant working group.

My staff have been active in all of these initiatives and have been involved in discussions with the telecommunications industry, Government departments and, regulatory bodies, as well as with other data protection authorities.

(m) Document Image Processing

From time to time it is necessary to consider the application of the Data Protection Act to new technologies that had either not been developed or were only in their infancy when the Act was adopted by Parliament in 1984. Document Image Processing (DIP) is such a technology and is based on the use of optical discs to store images of documents. One twelve inch optical disc can hold the equivalent of 200,000 A4 pages of text. Systems can range from stand-alone electronic filing units to fully networked/mainframe-linked applications. Indexing facilities and automated retrieval of documents are standard features whereas some systems have additional capabilities such as a facility to enter text via a keyboard.

The documents in a DIP system may include such as completed forms, correspondence, reports, notes, or records of telephone calls. There seems no doubt that information in such documents can fall to be personal data within the scope of the Data Protection Act. Data users will need to ensure they comply with the Data Protection Principles in relation to this personal data.

It is not always easy to see practical ways in which the Principles can be applied. For example, there may be no easy way of removing an item of irrelevant, inaccurate or out of date information which is simply recorded as part of what is, in effect, a photocopied document containing further items of information which remain in compliance with the Principles.

I am examining the issues raised by DIP systems with a view to giving guidance to data users.

3 The European Commission's Draft Directive on Data Protection

Last year, I reported the intention of the Commission of the European Communities (CEC) to publish a Draft Data Protection Directive. In July 1990, the Commission communicated to the Council of Ministers a package of six proposals which included such a Draft Directive and a specialised directive dealing with telecommunications. Some comments on developments in telecommunications are included in Section 2. This part of the report considers the Draft Data Protection Directive (1).

This major initiative by the CEC would harmonise data protection legislation in the European Community (EC) by, in effect, providing a strict and comprehensive data protection law to be followed by each Member State. The proposals are part of the preparation for the advent of the single market on 1 January 1993 and are proceeding under Article 100A of the Treaty of Rome. The Draft Data Protection Directive has aroused considerable debate and intensive lobbying.

Much effort has been devoted by my Office to understanding the proposals, explaining them to others and commenting to the Home Office and the CEC with possible revisions. In November, the Deputy Registrar visited CEC officials in Brussels and attended a CEC consultation conference. He has spoken to conferences of the Confederation of British Industry, the European Business Foundation and the National Computing Centre and he and my other senior staff expect to address further meetings on this issue.

The Data Protection Commissioners from countries in the European Community have met three times to consider the Draft Directive with a view to commenting collectively, where appropriate, to the Council of Ministers, the CEC and the European Parliament. A common view has been reached on some parts of the Draft Directive, but others still remain to be considered. There may, of course, be occasions when views will differ.

I have published some papers on the Draft Directive, including a possible restructuring of it, as a contribution to the debate. These papers are included in Appendix 1.

Decisions on the final form of the Directive will ultimately be taken by the Council of Ministers and a committee of officials from Member States is currently considering the draft. It is not at all clear at this stage that the final product will look the same as the initial proposals. Timescales, too, are uncertain although it seems sure that the Directive cannot be approved in time for all Member States to take the necessary measures to apply it by 1 January 1993.

The Draft Directive sets out two objectives. Firstly "the protection of the privacy of individuals in relation to the processing of personal data contained in data files". Secondly, to ensure that "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons to do with the protection afforded (to individuals)". In addition, the Draft Directive seeks to harmonise data protection legislation within the EC at "a high level of

(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

equivalent protection". The "exercise must not have the effect of reducing the level of protection already afforded in the Member States".

The Draft Directive, as originally proposed, would have a significant effect on the Data Protection Act. It introduces the concept of privacy which is not used in the Data Protection Act; would give greater knowledge to individuals about how information about them is used; would give greater control to individuals over the collection and use of that information; and would introduce compensation rights much wider than those currently in place. The result would be to provide enhanced protection for individuals.

This position of change and enhancement of existing legislation may not be unique to the United Kingdom. There are seven countries in the EC which have now ratified the Council of Europe Convention on Data Protection. Two countries have set up their own specific national legislation with a view to ratifying the Convention. Each country's legislation varies in its scope and style. As the Draft Directive seeks to harmonise at the highest common factor of protection for individuals, so each existing piece of legislation will find itself having to incorporate features from other legislation.

So far so good; enhanced protection for individuals which will be welcomed by many. However, the variations between the different national legislations are not there simply by chance. They often reflect different national approaches to law and different national backgrounds of concern. The problem when all these different facets are combined in one binding Directive is that they may not chime with any one nation's requirements. It is for this reason that I have suggested some changes to the structure of the Draft Directive which will, without losing sight of the need for common standards, allow greater flexibility for nations to fit matters within their own national outlooks and characteristics.

Leaving aside the issue of flexibility, there are some aspects of the Draft Directive which appear to go too far; to be too bureaucratic; or too onerous without balancing benefit.

An example of the first of these is the extensive application of the Draft Directive to manually processed data. In this country, we have approached the introduction of individuals' rights in respect of such data on a piecemeal basis. For instance, from 1 November 1991 there will be a right for individuals to see copies of their manually processed medical records, which parallels the right given under the Data Protection Act to access to these records when they are automatically processed. Whether these developments are proceeding widely enough or fast enough is not a matter for me; but the "rifle shot" approach, selecting sensitive areas for the introduction of data protection legislation in respect of manually processed data, does seem a sensible way to move forward.

I feel that there is an element of unnecessary bureaucracy in the registration (or "notification") scheme proposed by the Draft Directive. In 1989, I recommended to Parliament that the registration procedures in the Data Protection Act should be simplified. An Interdepartmental Committee set up by the Home Office last year recommended that registration should be ended. The proposals in the Draft Directive seem to move in the opposite direction to both of these recommendations. It would be helpful if these proposals could be reviewed and simplified.

Some procedures put forward in the Draft Directive appear to lead to requirements which seem to be unnecessary or without significant benefit. I have in mind the general need to notify individuals whenever information about them is communicated to a third party. This could certainly be of value in certain circumstances, but framed as a general requirement it seems likely to lead to some unnecessary work for data users and annoyance to data subjects.

There is one other aspect of the Draft Directive on which I would like to comment. As it stands, the Draft Directive allows for the development of European

"codes of conduct" which could be endorsed by the European Commission. It is important that the role and status of these codes of conduct is fully understood. Assuming, as I believe is intended, that they are to be equivalent to the codes of practice developed in the United Kingdom then I see no problem. These codes of practice do not in any way usurp or displace the statutory regulation contained in the Data Protection Act 1984. Rather, they provide helpful educational support for statutory regulation. If, on the other hand, the codes of conduct turn out to be a form of self-regulation which takes the place of statutory regulation, then there is cause for concern. I do not see how the high standard of protection which the Draft Directive seeks to establish for individuals, or a "level playing field" for trade could be properly, effectively or sensibly set up on a self-regulatory basis.

In conclusion, I welcome the Draft Directive and the regard it has for the protection of individuals; but there are problems with it which will need ironing out. No doubt discussions over the next year to eighteen months in the Council of Ministers' Committee will be complex and no doubt considerable lobbying by interested groups will continue. One thing seems fairly sure, the recommendations I have made for changes to the Data Protection Act, together with those from the Interdepartmental Committee, will have to take a back seat whilst consideration of the Draft Directive takes place. In the light of this, it now seems unlikely that the Data Protection Act will be changed for a few years.

4 Appeals to 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 first 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 apellant 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.

This year has seen the first hearings and decisions of the Tribunal. The hearings have concerned two subjects—the collection and holding of information for the community charge; and the extraction of third party information from credit reference agency files. In the latter case, action has been taken against five credit reference agencies and only one of the appeals has yet been determined. This section limits itself to those appeals where the Tribunal's findings have been published.

(a) Appeals by Community Charge Registration Officers

Four appeals were made and the cases were heard in September 1990. One Community Charge Registration Officer (CCRO) made his case by written representations. The appeals by the other three CCROs were consolidated and were dealt with by an oral hearing in which representations were made and evidence presented both by the CCROs and myself.

In its decision letters the Tribunal dealt with a number of points specific to the facts of the cases and particularly to the statutory role of the CCRO. These are unlikely to be of general interest to data users. However the Tribunal also dealt with and considered some general points, notably on the Fourth Data Protection Principle and my approach to enforcement which will be of interest

to all data users and these are explained below. The Fourth Principle states that "Personal Data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes".

The notices served on the CCROs for the South Northamptonshire District and the Runnymede and Harrow Boroughs alleged that holding a description of the type of property a chargepayer lived in was irrelevant and excessive to the purpose of the Community Charge Register. The notice recognised some exceptions, for example where the description is an integral part of the address, as in "The Cottage, Acacia Road". The notices required that the property type information should be erased unless it fell within one of these exceptions.

The notice served on the CCRO for Rhondda Borough alleged that the holding of date of birth information was irrelevant and excessive to the purpose of the Community Charge Register except in particular circumstances, for example where it was needed to distinguish individuals with the same name living at one address.

In its decision on the property-type information the Tribunal upheld my view in the following terms:

> "by continuing to hold property type information so widely and generally and without seeking to identify any small proportion where it might be appropriate there is clearly a holding of personal data which is irrelevant and excessive."

It was suggested in the course of the hearing that there might be further changes to the law governing the community charge. However, the Tribunal went on to comment generally that:

> "it is not relevant and would be excessive to hold wide classes of data merely on the ground that further changes in the law may in remote and uncertain future circumstances require further property types to be added to the existing exceptions identified by the Data Protection Registrar."

The Tribunal endorsed the general guidance given in Guideline 4 at para 4.2. This suggests matters which data users should consider in order to answer the question whether personal data are adequate, relevant and not excessive for the purposes for which they are held. The Tribunal endorsed the advice:

> "that the data user should seek to identify the minimum amount of information about each individual which is required in order to properly fulfil his purpose and that they should try to identify the cases where additional information will be required and seek to ensure that such information is only collected and recorded in those cases."

The Tribunal rejected a submission that the property descriptions were not personal data.

In addition to considering whether the information held was in breach of the Fourth Principle the Tribunal went on to consider my approach to the use of the enforcement powers. In particular, I had followed the procedure of serving Preliminary Notices on a number of CCROs warning them that I considered holding of property type to be excessive and stating my intention to take enforcement action or refuse registration. The Preliminary Notices invited the data users to make representations as to why notices should not be served. In considering the representations I took account of those made by all CCROs before coming to a final decision in respect of each particular CCRO. The Tribunal rejected the argument that this resulted in prejudice to the appellants.

The Tribunal was satisfied that I had properly taken into account the question of whether the contravention had caused or was likely to cause any person damage

or distress. The Tribunal also found that the Registrar was entitled to exercise his discretion to take action even where he concluded that there was no evidence of damage or distress.

The Tribunal decided that, given there was in this case a wide and general holding of excessive information, I had exercised discretion correctly in requiring its removal; although had the contravention only related to a trivial few items of information there might have been a case for exercising discretion differently.

The Tribunal dismissed the appeals.

In its decision in the Rhondda case which related to holding date of birth information the Tribunal applied the same tests and approach. Additionally it rejected the submission made by the CCRO in that case that the fact that information was obtained from answers *voluntarily* given on the canvass form and not under statutory compulsion, affected the question of compliance with the Fourth Principle.

The Tribunal dismissed the appeal.

(b) Appeals by Credit Reference Agencies

The Tribunal has now heard appeals in respect of all except one of the credit reference agencies against which enforcement notices were issued (see Section 6). However, by the closing date for this Report (31 May 1991), the Tribunal had only given a decision on the first of the Appeals. This was a joint appeal by CCN Systems Ltd and CCN Credit Systems Ltd (CCN).

The enforcement notice served on CCN alleged that the agency was processing personal data unfairly (in contravention of the First Data Protection Principle) by extracting information about other people who lived or had lived at the same or similar addresses as the applicant for credit when carrying out a credit reference search. The notice required that the agency should alter its method of processing by 31 July 1991.

CCN appealed on the grounds that the processing was not unfair, but even if it were unfair, I should have exercised my discretion differently, for the following reasons:

- that the processing would only be unfair if information were processed to produce inaccurate or misleading results;
- alternatively the Registrar was wrong to have regard primarily to the interests of the individual applicant for credit and the processing was fair having regard to the interests of lenders and borrowers generally;
- that it was fair because the information about other people (referred to as Third Party Information or TPI) was statistically predictive of credit risk, and equivalent to the use of statistics derived from information about others as practised in connection with insurance;
- that in any event it could not be proved that the presence of third party information had led to refusal of credit in any individual case.

CCN submitted that I should not have had regard to credit granting practices in other jurisdictions and further, if the notice were to be upheld, the period of time for complying with the notice was not sufficient.

I presented evidence of the complaints I had received; of how I had tried to change the credit industry practices; and why I had eventually decided to take enforcement action.

CCN presented evidence from its Managing Director and a number of its customers explaining the reasons for extracting third party information and the

effects on the lending industry if it were prevented from doing so. Both sides called evidence from expert witnesses on the statistical arguments.

The hearing lasted for 5 days and the Tribunal delivered its written decision some 8 weeks later.

The decision was a long and detailed one. It covered a number of points which are of significance in showing the Tribunal's approach to the interpretation of the Act as well as to the specific circumstances of the case.

The Tribunal set out the relevant law and summarised the arguments advanced to it by each side before making its findings. In dealing with the term 'processing' the Tribunal concentrated on the "extraction" of information which was the central issue in the case. It rejected the argument that the issue concerned was the use of the information, which would not be covered by the First Principle. It also rejected CCN's argument that personal data should only be regarded as extracted unfairly if inaccurate or misleading information were extracted. It took the view that in this case the activity of extracting the information by a complex computer program was processing within the terms of the Act and could be unfair.

The Tribunal then considered whether the processing in question should be regarded as unfair and found:

> ". . . in our view the program instructing the machine can be unfair if it is deliberately designed to extract certain information for the registered purpose. The unfairness, if there is unfairness . . . lies in the instructions to extract for the purpose of credit reference . . . material irrelevant to the individual who is the subject of the credit reference."

It then delivered its view of whether the processing carried out was in fact unfair. The Tribunal stated that:

> "having regard to the Act as a whole and in particular . . . the Data Protection Principles set out in Schedule 1 . . . the purpose of the Act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied rather than those of the data user."

and

> "in our view in deciding whether the processing we have described is fair we must give the first and paramount consideration to the interests of the applicant for credit—the 'data subject' in the Act's terms."

Applying this approach the Tribunal came to the conclusion that it was unfair to the individual to program the extraction of information so that on a search for credit assessment it produced information on people with whom the individual had no links or no financial relationship. It found this despite the fact that it was satisfied that third party information had predictive value. It accepted that CCN did not intend to process data unfairly but endorsed the view that the question of fairness is one to be determined objectively.

On another point the Tribunal decided: "we do not consider a comparison with insurance advances CCN's case".

In its findings and approach to the law therefore the Tribunal endorsed my view on all the relevant points.

The Tribunal then went on to consider how I had exercised my discretion in this case. It pronounced itself satisfied that the system of processing had led to distress for a number of people and that I was right to take this into account in

deciding whether to issue a notice. However, the Tribunal considered that the enforcement notice should have distinguished between different sets of circumstances instead of forbidding the extraction of third party information in all cases. It therefore amended the notice and added provisos to it.

One area of concern to the Tribunal was that what had been described as third party information might in fact be information about the same person. The Tribunal accepted there could be problems with matching information given on an application for credit with information on the database. It, therefore, added a proviso (a) that allowed the extraction of information in circumstances, for example, where information was recorded under a similar name and initials to the credit applicant at the same address at the same time of residence.

The Tribunal then went on to consider the extraction of information about people:

> "clearly not the subject, who share the same surname as the subject and who might be members of the same family living with the applicant as members of a single household".

It pointed out that information about the credit status of a member of an individual's immediate family might be relevant to the individual on occasions. However, it would not be possible to form a judgement on this without extracting the information. It therefore added a specific proviso (b) to the notice which would allow the extraction of information about individuals with the:

> "same or similar name who are reasonably believed to live as members of the family of the subject in a single household".

It extended this to cover family members with a different surname in a further proviso (c), but made clear that this did not allow a search to extract information on individuals with another surname as a matter of routine, but that this could only be done on individuals who:

> "on the basis of information obtained before such processing, are reasonably believed to live as members of the family of the subject in a single household."

The Tribunal went on in the light of the evidence it had heard to vary the time for compliance with the notice and allowed the agencies until 1 January 1993 to comply.

(c) Appeal to the High Court

After carefully considering the Tribunal's decision in the CCN case and taking further advice from leading counsel, I have appealed to the High Court. Two main grounds of the appeal are that:

- the wording of the proviso imposed by the Tribunal is ambiguous and as it stands it would still allow information to be extracted which has nothing to do with the individual applicant for credit; and
- the Tribunal had heard no evidence on which it could decide that the financial standing of other people who lived in the same household as the applicant was relevant to his or her creditworthiness.

CCN has cross-appealed against the findings of the Tribunal.

No date has yet been set for the hearing of the appeal in the High Court.

(d) Advice for Data Users

As mentioned at the beginning of this Section, I publish advice to data users through a series of Guideline booklets. The Tribunal's views on the law, given

so far, are entirely consistent with those taken by my Office and contained in the current Guidelines. However, the Tribunal sometimes expands on the views in the Guidelines.

As a view of the law is developed, and subsequently modified or confirmed by the Tribunal or the Courts, the Guidelines will be added to or amended. However, additions and amendments cannot be immediate and it may be helpful to data users now to extract a number of the more general points from the decisions given by the Tribunal and cross-reference these to the Guidelines. These general points are:

1. In deciding whether a data user has complied with the Data Protection Principles the test is an objective one. The intention of the data user is not relevant. (Guideline 4: page 12, paragraph 1.11).

2. In considering whether to take enforcement action the Registrar must consider whether damage or distress has been caused to any individual and he may properly decide to take enforcement action even where there is no evidence of damage or distress. (Guideline 7: page 6, paragraph 2.5).

3. In assessing "fairness" under the First Data Protection Principle paramount consideration is to be given to the interests of the individual data subject, not the interests of the data user. (Guideline 4: page 4, Introduction, Lines 5-10; page 8, paragraph 1.4, lines 1-2; page 11, paragraph 1.10).

4. In considering where information is excessive under the Fourth Data Protection Principle the Tribunal confirmed that where a category of information only relates to a few individuals it should only be held in respect of those persons. (Guideline 4: page 16, paragraph 4.2).

5 Complaints from Individuals

Last year I reported that complaints had risen very sharply from 1122 in the previous year to 2698. This year the number of complaints has fallen away to a total of 2,419. The principal reduction has been in the number of complaints about unsolicited mail.

The pattern of complaints has again fluctuated. For example, consumer credit complaints ran at 17% of all complaints received last year, yet in the year before that they were 35% of complaints. This year, consumer credit accounts for 31% of all complaints. Complaints about the subject access requirements of the Data Protection Act, which had fallen from 18% in 1989 to 8% last year have now increased slightly to 9.5% this year. Unsolicited mail complaints, having seen a dramatic rise last year to 45% of all complaints, have now dropped back to around 31% of all complaints I receive.

It may be some time before any stable pattern appears for either the volume or nature of complaints. However, there has been a recognisable shift this year towards the more complex complaints which require greater effort to resolve. It may be that data users are now more readily settling the routine complaints without individuals having to resort to my Office. In earlier years, a significant number of complaints were from frustrated individuals who had received no reply or an inadequate reply from organisations to which they complained. This sort of complaint has reduced in volume.

Despite the trend to increased complexity in complaints, there have been improvements in productivity during the year. To a large degree, these have arisen from the increasing knowledge of complaints staff, for example, about the operating procedures of data users. One result is that over 60% of complaints can now be handled without the need for detailed investigation.

The number of complaints unexamined at the end of the reporting year has dropped from 310 last year to 112 this year. However, there are currently 522 open complaint case files. Present experience is that 36% of all complaints are completely dealt with within three months and 67% within six months. But there is a hard core of about 9% of complaints, being those which are more complex or novel, which take over a year to resolve.

Last year I reported that regional investigating staff were being used, where necessary, to interview complainants and get a detailed statement of the complaint. With complex complaints this approach can be particularly helpful to complainants who may have a very scanty knowledge of data protection provisions and the rights the Act gives to them. In some cases, regional staff are also able to follow through and seek to resolve a complaint by discussion with the data user.

Some examples of complaints are:

Case 1

The complainant had encountered problems with her credit reference file. The financial dealings, including several debts, of a local company had been added to her file because they had wrongly been given her post code. The complainant

wished to disassociate herself from the company involved. She also felt that this information had been the reason for her being turned down for credit. However, when she approached the credit reference agency they refused to remove the offending information.

The complainant was advised to have a notice of correction added to her file which would indicate that she was not financially responsible for the company in any way. This notice was added to the credit reference file although the County Court Judgements held against the company still showed her post code.

The credit reference agency was then warned that the way such data was held was in breach of the Fourth Data Protection Principle. This was because the personal data were inadequate and irrelevant for the purpose of providing details of the complainant's credit worthiness. The credit reference agency agreed to remove the judgements in the name of the company from the complainant's file.

Case 2

The complainant was concerned about receiving direct mail from an organisation. Attempts were made to get this stopped, but he continued to receive mailings.

Formal action was considered necessary to remedy the situation and the Registrar served an enforcement notice for contravention of the First and Fourth Data Protection Principles. The First Principle was breached because the company had unfairly processed personal data relating to the complainant resulting in the despatch to him of unsolicited promotional literature despite his requests to the contrary. Also, the Fourth Principle was breached because the data user held personal data which were inadequate in relation to the purpose for which they were held. This was because they were not marked so as to ensure that such literature would not be despatched against the complainant's wishes. The data user did not appeal against the notice.

However, despite this, a further mailing was sent to the complainant. The data user was then prosecuted for failing to comply with the enforcement notice. The data user pleaded guilty and was fined as well as being ordered to pay prosecution costs.

Case 3

The complainant had exactly the same initial and surname as her husband. She and her husband left a particular community charge authority area. A month later she received a reminder from the authority that two months instalments of her charge had not been paid. On making enquiries of the authority she found that her husband's account had been credited with the same amount by which hers was underpaid and was told that a transfer would be made. Despite having received this information, the following month she received a final demand for the unpaid instalments. The complainant was concerned that the authority held inaccurate data about her and had divulged information about her husband's community charge account to her as a result of her telephone enquiry.

The authority explained that the errors in the accounts had occurred because the complainant's husband's direct debit slip bore an invalid account number. The authority asked the bank to change the number, but did not clearly stipulate whose account was to be changed. The bank changed the number but on the complainant's account which, until then, had been correct. Subsequently, therefore, the complainant's payments were being automatically transferred to her husband's account. This error was corrected and the authority provided a satisfactory explanation about the measures in force to ensure it did not make unauthorised disclosures over the telephone.

Case 4

The complainant stated that information from the Community Charge Register had been disclosed to a central government department. The Community Charge Registration Officer admitted that this had occurred as a result of a misunderstanding. Steps were taken to retrieve the information and the procedures were reviewed to ensure a similar mistake would not recur.

Case 5

The complainant had been refused credit and had obtained a copy of her credit reference file. On it she had found details of a County Court Judgement at her address in the name of her father. The complainant maintained that her father had never lived at that address; she did not know his whereabouts and only seldom heard from him. She contacted the creditor organisation which acknowledged that the debt was not hers. They also advised her that a former friend of her father had given them her address.

The Registrar was satisfied that the father had never lived at the complainant's address and advised the credit reference agency that it was holding data in contravention of the Fourth Data Protection Principle. Information about the complainant's father's judgement filed against her address when he had never lived there was irrelevant and inadequate for the purpose of providing information about the financial status of either party. The agency agreed to remove the judgement details from the complainant's file and to advise all users of the file within the previous six months of the deletion.

Case 6

The complainant was refused credit and obtained her credit reference file from one of the credit reference agencies. On her file she found a County Court Judgement in a name which, although there were no initials, could have been that of her husband or her son.

The complainant contacted the creditor organisation which confirmed that the Judgement related to the son and was in respect of unpaid charges for services provided to him and his ex-wife at their former matrimonial home. The complainant suspected her former daughter-in-law of giving her address even though her son had only stayed there for two days during his divorce.

The creditor had contacted the three major credit reference agencies and they had asked that the complainant should arrange with them to have a Notice of Correction placed on their files. The creditor also notified the Court, but apparently this sort of correction is not passed on to the central register of County Court Judgements.

The Registrar advised the credit reference agency from whom the complainant had obtained her file that, as she had challenged the accuracy of the information received by them from a third party, the challenge should be recorded or the information removed from its database. The credit reference agency confirmed the information had been removed. On checking with the two other major agencies it was found that the entry had also been dropped from their files.

Case 7

The complainant purchased a washing machine from a high street store and was asked to complete an application form for credit. Details from his application

form were entered into a computer and he was horrified to find the personal details, which he provided on the application form, were displayed on a VDU positioned about 6ft high on a shelf and clearly visible to the other customers in the store. He complained to the store manager and subsequently to the Registrar.

A regional investigator visited the complainant and the store. Although the position of the VDU in that particular store had been changed, it appeared that there was a problem in other stores. It also appeared that staff generally were not aware of their obligations under the Data Protection Act.

The company reviewed the location of all VDU's in its stores and found that there were a number where information could be read off the screen by the public at large. The company was in the process of replacing computer equipment and assurances were given that the position of the new VDU's will ensure compliance with the security requirements of the Eighth Data Protection Principle. The company sent gift vouchers to the complainant in recognition of the embarrassment caused to him.

Case 8

The complainant received a time share mailing addressed to her husband who was serving in the armed forces. The complainant was particularly concerned about the security aspects since the mailing was addressed to a relative's home which was used as an accommodation address.

The timeshare company had obtained the name and address from a database company which computerises the electoral register. The complainant's husband had arranged for the relative to have a proxy vote in his name and consequently his name appeared on the electoral role at the relative's address. The details of the complainant's husband were suppressed by the database company.

Case 9

The complainant was receiving unsolicited mail as a result of enquiring about the products of a mail order company. Upon investigation it became apparent that the company to whom the complainant had originally enquired, had sold its customer list to another similar company. The customer list was subsequently made available to other companies on behalf of the new list owner, by a list broker.

The company that had purchased the list was, at that time, only registered under the Data Protection Act as a Computer Bureau. The Registrar prosecuted the company for holding personal data while not being registered; the company pleaded guilty and was fined.

Case 10

The complainant was refused credit and applied for a copy of his file from a credit reference agency. The file contained details of a County Court Judgement against a neighbour. The address on the judgement was incorrectly recorded as the complainant's address. The complainant wrote to tell the creditor of the mistake. When he received no reply he complained to the Registrar.

On investigation, the creditor admitted the error. The creditor then informed the credit reference agency concerned, and the court. The County Court Judgement was removed from the complainant's credit reference file.

Case 11

The complainant had received forty-three unsolicited letters from a charity. Each letter had a slightly different version of the complainant's name.

The source data was traced back to a small mail order gift company. The company explained that the complainant must have been the victim of a hoax, in that coupons had been completed in the individual's name which the company had recorded in good faith, considering them to be separate individuals. The mail order company removed all the versions of the name from its database.

Case 12

The complainant hired a car from a United Kingdom rental company for his holidays abroad and was given a hire voucher. The foreign representative stated that the voucher value exceeded the car hire charge and that a refund was due to him.

After returning to the United Kingdom, the complainant started receiving payment demands from the rental company. There was clearly a discrepancy; one of the computerised documents indicated that the complainant had been overcharged and other documents indicated that he owed money to the rental company.

After investigation, the rental company agreed that an error had occurred. The false invoices were cancelled and the rental company apologised to the complainant for the inconvenience caused.

Case 13

The complainant and his colleagues were advised that, according to a government department's records, payments due from employees of their company had not been made. The complainants' employers confirmed that the necessary deductions had been made and sent to the relevant department. The complainant was concerned that he and his colleagues might be denied benefits due to an error in computer records at the department.

After lengthy investigations the department found that the delay in crediting the payments was due to a rejection of the reference number quoted by the complainant's employers. The department corrected the reference number and the records of complainant and his colleagues were updated to show the corrected details.

Case 14

The complaint concerned a large volume of mail which a minor (aged 10) was receiving offering her financial loans and prize draws. The girl's father asked the Registrar to arrange the removal of his daughter's name from the relevant mailing lists.

The father supplied some examples of the mail received and these were used to trace the mailing lists. It was discovered that, as a joke, a guarantee card seeking lifestyle information had been completed in the child's name by one of her cousins and this was the reason why her name was on various mailing lists. The list owners confirmed that complainant's daughter's name had been removed from their mailing lists.

Case 15

Complaints were received concerning direct mail from the United States of America. The mailings advertised the services of many diverse companies but were identified as emanating from one source in the USA. The mailing lists originated in the United Kingdom and were traced to two companies. Both companies collected names and addresses via coupon advertisements in newspapers and magazines.

Having regard to the nature of the mailings, which were under investigation by American postal authorities, it was concluded that the transfer of the mailing lists to the United States was likely to lead to contraventions of the First, Second and Seventh Data Protection Principles.

A Transfer Prohibition Notice was issued against one of the United Kingdom companies and the second company provided a written undertaking that it had no intention of conducting any further business with any of the corporations named in the prohibition notice.

Case 16

The complainant had lost her medical card and needed to register with a new doctor. Her local Family Health Services Authority issued a new card for her. The complainant had learnt her NHS number by heart as a child and felt sure that the number on her new medical card was wrong.

Following investigations, the complainant received an apology and was issued with a new card showing the correct NHS number.

Case 17

The complainant purchased an item from a department store and paid by charge card. The next day she spotted the same item on sale at a lower price. She was advised by the store to pay again at the lower price and her card account would be refunded with the original purchase price. When the card account arrived it had only been credited with the difference between the two prices. The lady was out of pocket and complained to the department store.

Eventually her card account was amended to her satisfaction. Some time later the complainant applied for a charge card from another retail organisation. She was refused and advised to apply to a credit reference agency for a copy of her file. This showed that, while she had been disputing her card account, the department store had informed the credit reference agency that she had been late in paying her account.

The complainant contacted the store and her credit reference file was amended. Later she sent for her credit reference file from a different agency and saw that it contained the same error. She then complained to the Registrar. After the Registrar's staff contacted the department store the complainant received an apology, an assurance that all her credit reference files were now correct, and a gift voucher.

Case 18

The complainant was being sent reminders to renew a television licence although she had already obtained one. She had also been visited by the licensing authority's enquiry officers. With her complaint, she provided copies of her licence and the most recent reminders.

It was pointed out to the licensing authority that the postcode on the reminder was incorrect. The authority explained that the complainant's address details had become corrupted on its files; this caused reminders and the visit by the enquiry officers. The authority gave assurances that its records had been corrected and conveyed its apologies to the complainant.

Case 19

The complainant sent copies of distressing advertising material which had been mailed to his young daughter from an animal charity. He had written several letters and made telephone calls to the charity requesting that her name be removed from its mailing lists. However, she continued to receive the mailings.

The charity was asked to remove the young girl's name and address from their mailing lists. It replied assuring the Registrar that the daughter's name had been removed from all its lists and sent a letter of apology to the complainant.

Case 20

The complainant wrote on behalf of his father who was receiving letters from a mail order company addressed to his wife who had died two years previously. Shortly after his mother died, the complainant ensured that all amounts owing to the company had been paid and he also asked them to remove his mother's name as an agent and from all mailing lists. However, despite letters and telephone calls, the company continued to send catalogues and mailings to his father.

The mail order company was asked to ensure that the lady's name was removed from all lists owned or controlled by it. The company gave assurances that this action had been taken and offered apologies to the complainant and his father.

This case is actually one which falls outside the terms of the Data Protection Act which only apply to living individuals. However, a number of these complaints are received and it has proved possible to assist in resolving them.

Case 21

The complainant had purchased a television set by a hire purchase agreement and had always paid regularly. He received letters demanding payment of an outstanding debt for the television set, when the account had already been fully paid off. The letters had been sent from three different companies in the same group. He wrote to the companies telling them that he had paid his account in full and also made subject access requests to them. He did not receive satisfactory responses from the companies.

Following investigation, it transpired that the complainant's account had become confused with a fraudulent account. The companies corrected their records and apologised to the complainant. They also paid compensation to him and responded to his subject access requests.

Case 22

The complainant had made a subject access request to a local authority without getting a reply. Following investigation, the authority explained that the problem was due to an administrative error and apologised to the complainant. Assurances were given to the Registrar that the relevant personnel are now properly aware of the subject access provisions of the Act.

Case 23

The complainant was concerned about inaccurate information held by an organisation of which she was a member. She was a pacifist, yet her membership details had a reference to the armed forces and she was outraged about this.

The case was then taken up with the organisation concerned which explained that the mistake had occurred as the result of human error. The offending reference was deleted and the organisation gave a written assurance that the erroneous information had not been disclosed to any third parties.

Case 24

The complainant decided to purchase goods from a department store. He filled in an application form for the store's own credit card and was subsequently advised that he was not creditworthy. It transpired that the store had consulted a credit reference agency and received information about his son's debts.

Investigation showed that the decision to refuse credit was made because of the adverse information concerning the complainant's son. The store agreed to contact the complainant in order to give his application further consideration.

Case 25

An individual had written to an insurance company in reply to an advertisement for a personal pension illustration. When he received it the envelope also contained part of an illustration for someone else. This included their name, address and salary.

It was discovered that one of the despatchers who filled the envelopes for posting had placed both the personal illustrations in one envelope. The company expressed concern about this incident and said that they fully appreciated the serious consequences that could result from such information reaching the wrong hands.

They gave assurances that, in the future, spot checks would be made by supervisors before envelopes for despatch were sealed. In addition, employees would be reminded of the need for care and accuracy.

Case 26

The complainant was refused banking facilities and sent for her credit reference file. When she received her file she found it contained no adverse information about her or any of her family but there were entries containing adverse information about another person with the same name and initials as her who lived at a very similar address but in another part of her town. The file contained information about accounts in the joint names of the namesake and her husband.

Investigation confirmed that the credit reference agency's system was designed to produce this third party information. The complainant was advised to put a Notice of Correction on her file and told of the enforcement action the Registrar is taking to resolve problems arising from the use of third party information for credit assessment.

Case 27

The complainant was renting a video recorder from a high street store. He wanted to rent a television set as well and made the necessary arrangements with

the store. When the television set was not delivered, he telephoned the shop to find that the company had limited the monthly credit he was allowed and this was now less than he had been paying for the video recorder. When he applied for his credit reference file he found details in it of a written-off account in the name of the previous owners of his house.

As he had already arranged to have a Notice of Correction added to the file he was advised of the enforcement action the Registrar was taking to resolve the problems arising from the use of third party information for credit assessment.

6 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 the Crown Court, or their equivalents 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.

As I forecast in last year's Report, I have this year adopted a policy of publishing a named list of those against whom I have taken prosecution or supervisory actions.

(a) Prosecutions

Charges brought this year have fallen 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 6(5): Failure to keep the registered address up to date.

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

Section 5(2)(b): Knowingly or recklessly holding or using personal data for any purpose other than the purpose or purposes described in the register entry.

Prosecutions have been brought against 17 data users for criminal offences under the Act and a further 7 are awaiting hearing. The cases which have been concluded are listed in Table 1. In one of these cases the defendant has appealed to the Crown Court against the sentence imposed by the Magistrates' Court.

(b) Supervisory Actions

During the year Enforcement Notices have been served on five credit reference agencies—CCN Credit Systems Limited, CCN Systems Limited, Infolink Limited, Wescot Data Limited and Credit and Data Marketing Services Limited.

The first Transfer Prohibition Notice was issued on 30 October 1990. More details of this are given in (d) below.

Preliminary notices were served on three data users on 30 August 1990, in respect of breaches of the requirement under the First Data Protection Principle to obtain personal data fairly. The data users made representations as to why

Table 1: Prosecutions Concluded in the Year to 31 May 1991

Section of the Act	Data User	Court[1]	Date	Fine £	Costs £
5(1)	Pitman & Howard Ltd	City of London	04.06.90	400	400
5(1)	Success With House Plants Limited	Wells Street	04.06.90	350	500
5(1)	My Favourite Recipes Limited	Wells Street	04.06.90	350	500
5(1)	Michael J Walters t/a Walters Commercial Stationers	Peterborough	22.06.90	200	100
5(1)	Avon Direct Mail Services Limited	Long Ashton	27.07.90	250	100
6(5)	Caldmore Area Housing Association	Walsall	08.08.90	Absolute Discharge	
5(1)	Levi Strauss (UK) Ltd	Northampton	20.08.90	1000	50
10(9)	The Church of Scientology Religious Education College Inc	West London	27.9.90	500	250
5(1)	United Guarantee Plc	Clerkenwell	11.10.90	200	300
5(2)(b)	The Football Association Ltd	Marylebone	25.10.90	Conditional Discharge for 2 years	300
5(1)	WL Insurance Services Ltd	Croydon	04.12.90	400	564
5(2)(b)	Halifax Building Society	Leeds Crown Court	13.12.90	Jury directed to Acquit	
5(1)	The Spectator (1828) Limited	Clerkenwell	25.02.91	160	340
5(1)	Cheshire County Football Association	Northwich	27.02.91	200	400
10(9)	CCRO—Great Yarmouth Borough Council	Great Yarmouth	29.04.91	750	350
5(2)(b)	Leicester City Council	Leicester	03.05.91	1000	250
5(1)	Gala Air Holidays Ltd	Redbridge	15.05.91	400	300

(1) All cases were heard in Magistrates' Courts except for that against the Halifax Building Society which was heard in the Crown Court.

Enforcement Notices should not be served. Undertakings are currently being agreed which it is anticipated will resolve these cases.

In August 1990, 10 Registration Refusal Notices were served on individuals, companies and other organisations, where inadequate information had been provided on application for registration. A further 40 refusal notices were served in May 1991 on the same grounds.

(c) Cases before the Data Protection Tribunal

Data users receiving an Enforcement, De-registration, Transfer Prohibition or Registration Refusal Notice may appeal to the Data Protection Tribunal. In November 1990 the Tribunal met for the first time in order to consider appeals by four Community Charge Registration Officers (CCROs). The appeals were in respect of an Enforcement Notice which had been served on the CCRO of South Northamptonshire District Council and Registration Refusal Notices which had been served on the CCROs of the London Borough of Harrow, Rhondda Borough Council and Runnymede Borough Council. All the notices alleged the holding of irrelevant and excessive information collected from the community charge canvass forms. The Tribunal upheld my view that the holding of this information constituted a contravention of the Fourth Data Protection Principle. The CCROs subsequently gave me undertakings that they would remove the information from their computer systems. Further details of these Tribunal appeals and decisions are given in Section 4.

The credit reference agencies referred to above have appealed to the Data Protection Tribunal against the Enforcement Notices served on them. The joint appeal by CCN Systems Limited and CCN Credit Systems Limited was heard in January this year. The Tribunal upheld my view of the law, but concluded that I should have exercised my discretion differently in that the Enforcement Notice was too wide. The Tribunal added provisos to the original notice which endorsed the extraction of third party information in certain family situations. I have appealed the Tribunal's decision to the High Court and CCN Systems Limited and CCN Credit Systems Limited are jointly cross-appealing. A date for the High Court hearing is awaited. Further details of this Tribunal appeal and decision are given in Section 4.

The Tribunal has also heard the appeals by Infolink Limited and Equifax Europe Ltd (formerly Wescot Data Limited) and decisions on these cases are awaited. The appeal by Credit and Data Marketing Services Limited is to be heard during the first week of July 1991.

Also awaiting hearing before the Tribunal is an appeal by the Halifax Building Society against an Enforcement Notice issued on 9 February 1989. This concerns the right for an individual to have a copy of information held about him or herself by a data user. This right is set out in the Seventh Data Protection Principle. The hearing of the appeal was postponed until the prosecution of the Halifax Building Society had been heard at Leeds Crown Court. It is anticipated that the appeal will now be heard in the autumn.

(d) Transfer Prohibition Notice

A Transfer Prohibition Notice under Section 12 of the Data Protection Act was served on Winsor International Limited to take effect on 3 December 1990. The notice forbade the transfer of personal data held by Winsor International Limited, namely names and addresses of individuals, for the purpose of direct mail, to:

— the Astrology Society of America Incorporated;

— International Reports Publishing Incorporated;

— Harvard Square Lottery Symposium Incorporated;

— Lourdes Water Cross Incorporated;

— Win With Palmer Incorporated;

— International Marketing of the USA; and

— Mr Ben Buxton of New Jersey.

At the time of serving the notice, the United States Postal Service was seeking a Court Order in New Jersey to restrain the activities of Mr Buxton personally and of his corporations. The United States Postal Service alleged that Mr Buxton, directly and by his corporations, was defrauding consumers through false and misleading promotions of horoscope, lottery winning systems, religious trinkets and other products.

Promotions of horoscopes, religious trinkets and some other products had been verified as having been mailed to consumers in the United Kingdom and a number of organisations, including the Office of Fair Trading, had received complaints about them.

The mailings by the United States corporations would have breached United Kingdom consumer protection regulations had they been sent from within this country. It also appeared that the proceedings in the United States courts, even if they were successful would not necessarily stop Mr Buxton from mailing to consumers in the United Kingdom.

An investigation by my Office established that the names and addresses of consumers in the United Kingdom had been transferred to the United States by Winsor International Limited.

I was satisfied that the mailings in question were unlawful, being in breach of both United States and United Kingdom statutory regulations, and that the transfer of personal data would lead to the holding and processing of personal data for that unlawful purpose. I also considered whether individuals would be able to have access to the information about themselves once it was held as personal data in the United States.

I served a Transfer Prohibition Notice on the grounds that the transfer of personal data to the named United States corporations would be likely to contravene or lead to a contravention of the First, Second and Seventh Data Protection Principles.

(e) Monitoring and Promoting Compliance with the Act

During this year, I have begun to consider ways of monitoring and promoting compliance with the Act. Two exploratory initiatives have been undertaken. The result of these are still be be evaluated before decisions are made on future actions.

(i) *Fair Obtaining of Information for Direct Marketing*

In October 1990, my staff began considering press advertisements which appeared to seek information about individuals that might subsequently be held on computer. They are investigating any possible breaches of the "fair obtaining" requirement of the First Data Protection Principle. The relevant advertisers are sent a letter setting out their legal obligations in terms of registration and my view of the fair obtaining of information. The advertisers are also asked to complete a questionnaire about the uses and disclosures of information sought in their advertisements.

To date, one hundred advertisers have been approached, of which around one third have yet to be allowed a reasonable time in which to reply. Of the rest, twenty-one would appear either not to be data users at all or to make no uses of personal data other than to fulfil orders and to dispatch further marketing offers on their own behalf.

However, two companies are in the process of being prosecuted for non-registration offences and another ten organisations are being investigated. Thirteen companies have received comprehensive advice regarding the way in which the Act applies to direct marketing. My staff are in the process of negotiations with a further nine data users about remedial action in relation to personal data which was apparently unfairly obtained in the past and in these cases the outcome might yet prove to be formal enforcement action.

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

A survey was carried out in the City of Cambridge in May this year. Its objective was to determine whether there were computer users who had failed to register under the Act. There was extensive local coverage by newspapers, radio and television and considerable support by the town's public bodies.

The survey had two main parts: firstly a distribution of leaflets to 42,500 city centre addresses; secondly random visits by regional investigators to a range of organisations. The activity was designed to give assistance to those who should register, but who were genuinely unaware of this. However, those organisations which appear simply to have ignored the requirement to register are being considered for further investigation.

This experiment seems to point to one cost-effective way of raising awareness amongst data users, albeit it does involve an on-the-ground investment of staff time. The costs incurred have been more than covered by the extra registration applications received.

The conclusions to be drawn from an experiment of this nature are necessarily tentative. However, it appears that as many as one in four of the businesses visited probably needed to register, but had not done so. They were predominantly newly-established small businesses and may not be representative of all data users. Nevertheless, this experience underlines the work to be done in bringing the Data Protection Act to the attention of smaller businesses. This is referred to again in Sections 8 and 9.

7 The Data Protection Register

Almost 16,000 new registration applications were received during the year and the number of entries on the Register now stands at over 160,000. As a consequence of the three year registration cycle, the past year has been one of the quieter ones from the point of view of registration renewals. Even so, just under 20,000 applications have been received for renewal or for re-instatement of the details of an expired entry. In addition, there have been more than 24,000 requests to amend register entries. Data users visiting the Office's stand at exhibitions can now register on the spot with advice from staff on completing the applications forms.

A significant effort has been put into clearing the large number of registration applications which were held up with unresolved queries. Each of the data users concerned had been written to several times but without resolution of the outstanding issues. In the first six months of the year these suspended applications were reduced in number from 3,300 to 300. Some 2,570 of the cases were accepted onto the register; 300 were withdrawn by applicants who decided that they were no longer required to pursue their application; and 130 have been refused registration or are being considered for refusal.

The proportion of register entries which are not renewed has climbed from around 24% to about 30%. Some 2% of this increase has been caused by one organisation which has reduced its register entries from over 4,000 to 12. This organisation is not alone in reducing multiple register entries, although reductions by others are much smaller in size. Many of those who do not renew their registrations contact us to explain why they are not doing so; perhaps because the company has ceased to trade. Doubtless, a number of others have not renewed as they no longer need to be registered. However, a significant proportion appear not to renew their register entries even though registration is still required. A telephone survey of 1,000 randomly selected lapsed register entries has indicated that this proportion may be as high as 14%.

I had hoped, during this year, to complete work to provide access to the Register in public libraries via a Prestel service. The development is finished and the system is available for use in my Office. Unfortunately the financial pressures referred to in section 11 have made it impossible to offer the wider public service originally envisaged.

8 Informing People about the Act

In last year's Report, I stated that "there will be no further funds available for advertising after June 1990 until April 1991". This situation arose because of the television advertising campaign in the first half of 1990. Television advertising, even for the lightweight campaign mounted, is expensive and costs had to be recovered from two years' budgets. Hence most of the funds available for the financial year April 1990 to March 1991 were committed in advance and spent very early in that year. Unfortunately this funding problem is a continuing one for, as noted in Section 11, the approved level of grant-in-aid for 1991-92 is likely to reduce planned promotional expenditures for the coming year.

(a) Strategy

A rethink of strategy was, and is, clearly necessary. Such a rethink was also prompted by the research on public and data user awareness carried out in early 1990. More details of this (and the current research position) appear in Section 9, but broadly it showed public awareness of the Act increasing; awareness amongst larger data users remaining high; but awareness amongst smaller data users declining. These results were perhaps not surprising, bearing in mind that the strategy had been to direct publicity at data users in the early years of the Act and switch publicity to individuals after their rights came fully into being at the end of 1987. The volatility of the smaller company sector is also likely to have had some effect.

The strategy now is to divide activities more evenly between data users and individuals. Within the data user sector there is a further divide between obtaining awareness of the need to register and promoting compliance with the Data Protection Principles. In the light of financial restrictions main reliance is being placed on public relations work and a range of education and information activities.

Research in 1991 shows that:

- nearly all respondents from large companies are aware of the Data Protection Act; therefore the primary need here is for education about the Data Protection Principles;
- awareness amongst small companies of the need to register is still unacceptably low and needs to form the main thrust of the 'message' to them.

For several months now individuals and data users who telephone the Enquiry Service have been asked where they first heard about data protection. The results so far suggest that most data users first hear about the Act from their accountants, solicitors or computer suppliers. Promotional work in the past has included supplying advice packs to accountants and solicitors and leaflets to computer suppliers for their customers and it may be that this work is paying off. The results of these sorts of enquiries will assist in planning future promotional work.

(b) Activities

There have been about 1400 press mentions of the work of the Office or the Data Protection Act throughout the year. Many of these relate to the twenty-

seven news releases issued. Staff have given fifty-seven talks on the Act, sixteen radio and six television interviews.

It is not always the most apparently 'newsworthy' releases which receive the most coverage. For example, a short release reminding small businesses of the need to register ("Concern that Small Businesses May Risk Prosecution"), which was issued in August 1990 has been taken up by a wide range and number of newspapers and journals in the months since then.

The Home Secretary announced an increase in the registration fee with effect from 1 June 1991. To bring this to the attention of computer users, £45,000 was spent on a national press campaign and a small series of advertisements in regional business journals. A special fee increase notice was also produced for distribution at exhibitions and inclusion with relevant information from the Office.

A new edition of 'Update', a newsletter directed to computer users, was mailed at the end of March 1991 to some 142,000 organisations and individuals on the Data Protection Register. In addition a further 11,000 copies of the newsletter have been distributed through a wide range of representative bodies and other interested organisations. A major part of this Update addressed the issue of compliance with the Data Protection Principles.

Exhibition appearances continue to be a significant aspect of promotional activity and this year stands were taken at major computer shows in London, Birmingham and Scotland, plus 'specialist' shows such as the BMA Conference and the Exhibition on Healthcare Computing. The stands attracted nearly 10,000 visitors.

In Autumn 1990 my staff devised and presented a series of one-day seminars for the Direct Marketing Industry. They were run in conjunction with a professional seminar company which carried out all the marketing and administration tasks. The objective was to tailor advice and guidance to this specific sector and in particular to illustrate the requirements of the Data Protection Principles. The seminars were well supported, attracting over 300 delegates to four locations. Follow up research shows that they were also very well received. A new series will be mounted during the coming year for a wider audience encompassing the marketing and advertising sectors as a whole.

The new rights leaflet for individuals ("If there's a mistake on computer about you...") which was produced to coincide with the television campaign, continued to be heavily utilised through the year with over 43,000 copies dispatched by the Information Services Department.

The Guidelines and Guidance Notes also continue to be in strong demand with over 28,000 sets of Guidelines distributed throughout the year, together with 14,000 individual copies of Guideline 1 (An Introduction to the Act).

Finally, the Enquiry Service had another busy year, dealing with 40,445 telephone calls and 7,416 letters.

(c) Results

The gain in public awareness of the Data Protection Act (from 31% to 38%) shown following the television campaign in the first half of 1990 has been held in 1991. Although research showed that recognition of the advertising was not high (reflecting the lightweight nature of the campaign), it seems clear that it did create an impression with those who saw it and a greater understanding that there is a means of correcting computer errors.

The decline in the awareness of the need to register among small companies which hold personal records, evident from research in March/April 1990 has been reversed. Whilst awareness of this requirement (at 62%) still remains lower than in 1986 (70%), more general awareness of the Data Protection Act amongst these small companies is now higher (at 87% as opposed to 75%).

A fuller description of the various research results follows in Section 9.

9 Background Research

Research into public and data user awareness of the Act is carried out on a regular basis. At the same time, a picture is obtained of the public's concern about a wide range of issues including personal privacy.

Some results from the research carried out into public awareness and perceptions are given in Appendix 2. They cover the research programmes undertaken in February 1989, July 1990 and March 1991. The same appendix also contains information from data user research carried out in 1986, 1990 and 1991.

(a) Public Attitudes and Awareness

Public concern about protecting peoples' rights to personal privacy remains high. Some 70-73% of the public considered this very important across the three surveys. These figures fall below concerns about preventing crime on the streets (82-84%) and improving standards of education (73-78%) but are above concern about unemployment (58-70%) and inflation (56-62%).

Asked to rank the five privacy issues of most concern, the public rated "keeping personal information/details private" and "protecting the privacy of your own home/property" as equal first. Just over 70% of respondents are very or quite concerned about the amount of information that is kept about them by various organisations. The responses to these matters of privacy have remained constant over the three research programmes.

The total awareness of the Data Protection Act, including both spontaneous and prompted responses moved from 31% in 1989 to 38% in 1990 (following the television advertising campaign) and has held at 37% in 1991. Amongst those aware of the Act, there has been a steady, significant increase (55%-65%) over the three years in prompted awareness of an individual's right to see and correct information about him or herself. Over the last year, there has also been a statistically significant rise (64%-75%) in the number of people who think the right to remove information about themselves from lists or files is very important.

(b) Data User Awareness

For their part, data users are considered in two groups; small companies (less than 50 employees) and large companies (50 employees or more).

As might have been expected, there has been a significant increase since 1986 (31% rising to 45%) in the use of computers by small companies; especially the use of personal computers and word processors. The use of computers is directly related to size; 27% of establishments with 1 or 2 employees using a computer compared with 80% of establishments with 25-49 employees. All the large companies used computers.

The three sets of research results show that it is becoming increasingly common for personal records to be held on computer. This is true of small companies (25% rising to 43%) as well as large companies (72% rising to 97%).

Prompted awareness of the Act amongst small companies which hold personal records has varied from 75% in 1986 to 70% in 1990 and 87% in 1991. Similarly, awareness of the need to register amongst small companies has fluctuated from 70% in 1986 to 51% in 1990 to 62% in 1991. It was the low figure in 1990 which caused the rethink of strategy referred to in Section 8. Whilst awareness of the Act has remained constant (at 95%) amongst large companies holding personal records, even here there has been some decline in awareness of the need to register (96% dropping to 82%).

In both small and large companies holding personal records, awareness that there are other obligations stemming from the Act, for example meeting the Data Protection Principles, has remained constant. However, the awareness is low for small companies (26%) and not good (around 45%) for large users. Over the last year, the small companies have shown an increasing awareness that the Act confers rights on individuals (36% rising to 50%).

10 International Activities

Last year, I reported that international interest in data protection was developing rapidly. That trend continues; not only is there more European activity, but also increasing debate in the United States about the possible consequences of recent European Community data protection initiatives. There also appears to be a growing interest in developing countries. This section deals with international matters other than the European Commission's Draft Directive on Data Protection which is covered in Section 3.

(a) The Council of Europe

During the year the Committee of Ministers has approved a recommendation on the protection of personal data used for payment or other related operations and the report of a study on personal identification numbers. In addition,the Committee of Experts is currently looking at draft recommendations for the protection of personal data in telecommunications and in public files. Also, a Working Party is revising the existing recommendation on medical data banks and Working Parties have been established to look at the fields of insurance and of census and statistical data.

The 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data had, at the end of March 1991, been ratified by eleven countries, namely: Austria, Denmark, France, Germany, Iceland, Ireland, Luxembourg, Norway, Spain, Sweden and the United Kingdom.

Hungary and Czechoslovakia are now full members of the Council of Europe; Poland is an observer. It is clear that as part of a comprehensive revision of their constitutional and legal arrangements, each of these three countries is giving some prominence to data protection, which is seen as a significant human rights issue.

My staff have continued to attend the meetings of the Council of Europe Committee of Experts and they contribute to the New Technologies and Medical Data Working Parties of that Committee.

(b) The International Meeting of Data Protection Commissioners

In 1990 the Commissioners met in Conference in Paris. As part of those proceedings my Senior Assistant Registrar delivered a paper on "The Protection of Medical Data in Great Britain". I note with mixed feelings that as data protection activity expands internationally, the numbers attending these Conferences grow and proceedings have become more formal. There is now less opportunity for an informal exchange of practical experience between Commissioners. That will undoubtedly prompt further meetings of smaller groups of Commissioners and their staff to consider specific areas of interest.

The Working Group on Telecommunications and the Media has met three times in Berlin in the last year. It has concentrated its work on looking at the

Commission of the European Communities (CEC) proposed Directive on Data Protection in Telecommunications. My Senior Assistant Registrar has attended these meetings.

(c) Other International Contacts

Two of my staff attended a meeting with representatives of other data protection authorities to discuss issues relating to direct marketing. Also, I was pleased to welcome representatives of other European data protection authorities to a seminar organised by my office with the Advertising Association to study profiling in the direct marketing industry.

The Assistant Registrar, who is responsible for liaison with the Health Sector, attended the Third Global Conference on Patient Cards in Barcelona in March, 1991. The Senior Assistant Registrar gave a paper at an International Conference on Data and Consumer Protection in Telecommunications Services in the European Community in February, 1991.

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

My Office has, this year, received visitors and delegations from Australia, Belgium, Canada, Denmark, France, Germany, Guernsey, Ireland, the Isle of Man, Jersey, Kenya, Luxembourg, the Netherlands, New Zealand, Norway and the United States.

In October 1990 I visited the United States and met representatives of government, the private sector, consumer and civil rights organisations. It was a useful education on the developing use of personal data in the USA and of the legislative approach to privacy and data protection concerns. I was able, in turn, to brief American representatives on activities in the United Kingdom and on the CEC Draft General Directive on Data Protection.

Finally, the Data Protection Authorities of the countries which have ratified the Council of Europe Convention are required by that Convention to co-operate with each other. I am particularly grateful for the co-operation I have received in the investigation of cases with an international element. By way of example, one case required visits to France, the Netherlands and Denmark during which my investigators received every help and assistance.

11 Organisation and Finance

(a) Staffing

During the year, I have completed steps to change the balance of the Office, increasing the number of established positions and recruiting more senior staff to reflect the projected work programme for the coming years. I have agreed with the Home Office an increase in established positions from 70 to 89. These changes have meant that the Office is no longer running with long-serving staff with temporary contracts or in acting positions. Opportunities are being offered for part-time employment and about 13% of established staff now have contracts of this nature. In addition to established positions I have 16 regionally based staff who are paid per assignment.

(b) Financial Management Review

Treasury policy requires a review of the organisation, finance and staffing of non-departmental public sector bodies every five years. Such a review of my Office has been carried out in this year. My Office had a staff inspection, which is linked to the grant-in-aid conditions, in late 1987. I noted the very supportive conclusions of that staff inspection in my Fourth Report in June 1988.

Plainly another wide-ranging review in mid-1990 seemed very soon after the previous inspection. However, as I had just completed the Corporate View to 1993, and given the requirement for increased staffing, the timing was not unhelpful. The conclusions of the financial management review are the same as those of the staff inspection—that my Office is tightly complemented, well-organised and monitors and uses its resources effectively. The review supported my request for additional staff to meet additional workloads.

(c) Finance

Expenditure for the year, at £3.15 million was exactly the same as the amount budgetted. Receipts from registration fees for the year amounted to £1.94 million (against a forecast of £1.96 million). In addition, a further £0.12 million were received, principally from interest on funds in hand. The unaudited financial statements are given in Appendix 3. The audited account will be certified by the Comptroller and Auditor General and laid before Parliament later this year as required by the Act.

A word is appropriate on the financial situation in the current year. The grant-in-aid for the financial year to 31 March 1992 has been set at £3.42 million. This is an increase of 8.6% over the grant-in-aid for the year to 31 March 1991. On the face of it, this is satisfactory in terms of inflation, however the figure set is over £300,000 less than that I proposed which provided for identified growth in activities. The shortfall would have been greater than this, but the Home Office Division with which I negotiate the grant-in-aid helpfully transferred some funds to my Office from another budget.

These difficult financial situations, which can arise from time to time, are facts of life which have to be faced and I am seeking ways to reduce expenditure on

certain activities so as not to unbalance the programme of work committed or necessary. Regrettably, I may have to achieve most of the savings required by a sharp reduction in activity directed at informing the public and data users about the Act.

Unfortunately, the financial situation has been made worse by the recent increase in the rate of VAT from 15% to 17.5%. Since my Office does not add VAT to its charges and can not recover VAT payments, this increase will add an estimated £36,500 to running costs in 1991-1992. Even though the increased payment I have to make ultimately finds its way back to the Exchequer through the VAT system, the Treasury has apparently determined that extra grant-in-aid cannot be provided for this expenditure.

Following Parliamentary consideration, the Home Secretary has decided to increase the registration fee to £75 as from 1 June 1991. This increase is designed in part to recover past under-recoveries of costs, principally set-up costs, and in part to enable the Office to make progress towards achieving a cumulative break-even position over the next five years.

12 Conclusions

In my Annual Report in 1987 I discussed data protection as a new public policy taking its first steps in a complex society. I spoke of other public policies having to shift around in order to make room for the new arrival. Perhaps this year will come to be seen as the one in which this infant policy grew into a fuller role in public and political debate. This stems not only from developments in the United Kingdom but also from influences from the European Community.

The interest of the Home Affairs Committee of the House of Commons, illustrated in the discussion at its meeting on data protection in October 1990 and in its subsequent report, has been an important factor. The European Commission's Draft Directive on Data Protection has underlined the continuing concern to achieve a high level of protection for the privacy of individuals as one of the essential factors underpinning an open Community market.

The first appeals to the Data Protection Tribunal have been heard and determined in this year. More enforcement actions and appeals can be expected as implementation of the Act progresses. Tribunal decisions are an important stage in providing data users with more certain information as to how the law should work in practice. I am pleased that the Tribunal, on the arguments heard so far, has upheld the views of the law expressed in the Guideline Series published by my Office. That, in itself, should give data users greater confidence in those views.

With pressure from the Home Affairs Committee and support from Ministers, there is evidence that Government departments are more readily approaching my Office for comments on new legislation and developments. This Report highlights issues on topics as diverse as health, criminal records and child support. In the private sector, issues continue to arise related to personal finance and to direct marketing.

It is not only matters such as these that raise data protection questions. Developing technologies such as document image processing and communications present new and difficult problems. Extending the present legislation to cover manually processed records would also bring fresh challenges.

The failure to obtain the full grant-in-aid bid for 1991-92 may affect efforts to inform the public of their rights and data users of their obligations. However, the excellent conclusions from the Financial Management Review and the strengthening of the staff complement are both helpful in facing the many and diverse tasks ahead. The Office is neither crushed by nor complacent about these tasks, but remains in good heart.

Eric Howe
Data Protection Registrar

June 1991

Appendix 1

Papers on the European Commission's Draft Directive on Data Protection

This Appendix consists of three papers on the Draft Directive which have been made available from my Office. Papers A and B contain more general comments on the Directive and outline a possible change of approach to achieve the Draft Directive's objectives. Paper C re-draws the Draft Directive into a new form and includes suggested modifications.

All the papers have been produced as a contribution to the debate on the Draft Directive. The final format and content of a Directive is, of course, a matter for the Council of Ministers. The Draft Directive is being considered by a Committee of the Council of Ministers and by Committees of the European Parliament and the House of Commons. By Autumn of this year it is possible that these considerations will have caused significant changes in the Draft Directive as originally published. In that case, these present papers may well be out-dated and in need of review.

PAPER A—Prepared for the Meeting of EC Data Protection Commissioners at Wiesbaden, 30 November 1990

Data Protection in the European Community

Initial Views of the UK Data Protection Registrar

1. INTRODUCTION

1.1 The Commission of the European Communities has published a package of proposals on data protection in papers numbered COM(90) 314 final—SYN 287 and 288. This paper is a general commentary on the draft general directive within that package (SYN 287).

1.2 The United Kingdom Data Protection Registrar welcomes the EC Commission's initiative. Establishing rules about the lawfulness of processing, emphasising particularly the consent of the data subject, and the granting of specific rights to individuals would enhance the protection of individuals in the UK. The directive does present a number of practical problems flowing in part from its detailed and prescriptive nature. Those issues are looked at subsequently in this paper.

2. DO WE NEED THE GENERAL DIRECTIVE?

2.1 The Council of Europe Convention (Treaty 108) on Data Protection was opened for signature in 1981. Notwithstanding, resolutions of the European Parliament, recommendations of the Council of Ministers and Lord Cockfield's initiative, some EC countries have still not passed data protection legislation enabling them to ratify Treaty 108; they are Italy, Belgium, Greece, Portugal and Spain, although Spain has ratified the Convention in the absence of legislation.

2.2 Furthermore, even those countries which do have legislation, have legislated in distinctly different ways. The issue of whether one country gives equivalent protection to another has caused some difficulty leading to lengthy discussion between those countries who have ratified Treaty 108. Moreover, some data protection authorities will stop the transfer of data to a country which has data protection legislation and which has ratified the Convention but which in a particular case does not have the protection afforded by the law of the transmitting state.

2.3 If the EC is to consist of a single area in which persons, goods, services and information can move freely, then a single regime for data protection acceptable to all Member States would seem to be not only unavoidable but also desirable. Whilst there would seem, therefore, to be a need for a directive, the question remains open as to the scope and nature of the directive.

3. PRINCIPLES

3.1 The Draft Directive is clear about two matters. First, Article 1 requires Member States to ensure;

> "the protection of the privacy of individuals in relation to the processing of personal data contained in data files."

This is distinct from the UK Data Protection Act 1984 which states merely that it is "to regulate the use of automatically processed information relating to individuals . . .". No reason is given for the regulation. The

Directive gives the courts a yardstick against which to interpret the law, namely the protection of the privacy of individuals.

3.2 Secondly, the Explanatory Memorandum to the Draft Directive says that "the exercise must not have the effect of reducing the level of protection already afforded in the Member States". The reason given is that this type of legislation is intended to protect fundamental rights, and consequently the Draft seeks to harmonise by providing "a high level of equivalent protection".

3.3 A distinct point concerns the way the Directive goes about providing for data protection. There are in principle two approaches: to give specific enforceable privacy rights to individuals, or on the other hand, to set out an enforceable code of good information handling practice. The UK law tends to follow the second course with some elements of the first. The Directive has a 'belt and braces' approach reflecting its origin in the legislation of different member states and the objective of harmonisation at a high level. It sets out an extensive list of individual rights, but also embodies rules on the lawfulness of processing and in particular in Article 16 sets out quality of data rules drawn directly from Treaty 108.

4. Manual Data

4.1 The Directive would apply extensively to manual information. The UK Act regulates only those who process information "by equipment operating automatically in response to instructions given for that purpose".

4.2 The Draft Directive talks of "personal data . . . which, although not undergoing automatic processing, are structured and accessible in an organised collection according to specific criteria in such a way as to facilitate their use or combination". On reflection, however, this complex definition seems to restrict the coverage of manual data hardly at all. One's business desk diary of appointments seems to come within this definition.

4.3 An extensive application of control to manual records would seem to run the risk of multiplying conflicts with the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (Treaty 5) and in particular Article 10 of that Convention. A selective approach to the regulation of manual data might more successfully protect privacy interests whilst avoiding other conflicts of principle.

5. Significant Issues

5.1 *Will the Directive Change UK Data Protection?*

5.1.1 The Directive is complex and in some places written in unclear language. Some articles quote provisions of the law in particular countries. Other Articles refer to legal concepts appropriate to one country but either inappropriate or misleading in other countries. General principles are expressed to which there are often wide exceptions. Although it is still not clear what exactly the Directive means and the extent to which changes will be required in UK law, some aspects of the Directive should be commented on because of their general approach.

5.2 *Public and Private Sector—Lawfulness of Processing*

5.2.1 The Directive, unlike the UK 1984 Act, distinguishes the public from the private sectors. It goes on to prescribe the circumstances in which the processing of personal data will be lawful in those sectors. The UK Act

accepts that any processing is lawful if it is not prohibited by the general law and provided the data user has satisfied the procedural requirement of registering under the Data Protection Act. The Directive imposes some extra conditions. In the public sector, the principal rule is that processing is lawful if necessary for the functions of a public authority and, in the private sector, the consent of the data subject is the starting point. But it must be stressed that there are extensive subsidiary rules in both sectors. Examples are that a public authority may process data for a purpose other than that for which the file was created if authorised by a law conforming to the Directive, and in the private sector consent is not required if, amongst other cases, "the controller of the file is pursuing a legitimate interest, on condition that the interest of the data subject does not prevail". It is possible that the practical consequences for UK data users may not be as great as some have thought at first sight, but the Directive sets out the principle that there must be restrictions on the purposes for which personal data can be processed.

5.2.2 In the Chapter on lawfulness of processing in the private sector, the draft directive requires by Article 9 that, with exceptions, when a private sector body first communicates data to another person, the data subject must be told. This would be novel in the UK. It seems to flow from the view that there is little risk to an individual when information is kept within the original data user, but there is a significant risk when it is passed to another. The right to be informed would be a valuable extra right for individuals, but a more selective approach may be more appropriate and practicable than the sweeping form envisaged. It is particularly noteworthy that there is no duty to inform data subjects when a public sector body communicates with another such body. Those communications are permitted if they are necessary for performing the tasks of either public body. Unless the test of necessity were applied very strictly, this rule could readily permit extensive public sector data-matching.

5.3 *Registration*

5.3.1 The UK Data Protection Act creates a scheme of regulation around a registration system. Almost every data user has to register unless coming within a limited group of exemptions from the Act such as national security, purely personal purposes or payroll and accounts processing. In his 5th Annual Report to Parliament in 1989, the Registrar suggested that the present registration system should be revised. It seemed to impose too great a bureaucratic burden on small routine commercial enterprises who were not undertaking activities of major data protection significance. On the other hand, there seem to be definite benefits in having a list of the major and sensitive data users which can be used both for publicity and information purposes and also for enforcement activity. The Registrar proposed restricted registration of limited details by those data users who were judged by Parliament to be undertaking sensitive data protection activities.

5.3.2 The Directive proposes registration, but on a somewhat different basis to that put forward by the Registrar. The amount of information to be registered would be similar (but not identical) to that required by the present UK system, but only those data users who communicate personal data to others would need to register by notifying the supervisory authority. The directive uses the word 'communicate' rather than 'disclose'. That could mean something narrower than 'disclose' in the UK Act and so disclosures to agents for processing would not count as communication. Is 'communication' the correct trigger for registration? The UK Registrar still holds to the ideas put forward in his 5th Annual Report.

5.4 *Rights of Individuals*

5.4.1 The Directive requires individuals to be given by law a substantial list of enforceable rights. Some correspond to the UK law—e.g. the right of subject access. Some go further—e.g. rights of rectification or erasure of any data processed in breach of the Directive and rights to compensation for any damage arising from a breach of the Directive by a data user. Of particular note is Article 13 which sets out what an individual must be told when information is collected. It is similar to the view taken by the Registrar of what is meant by the fair obtaining of information, but is stricter and less flexible. One or two provisions of Article 14 are entirely novel in UK Law—such as the express right to have data erased from marketing lists and the restriction on purely automated decision making systems.

5.4.2 The marketing list right would apply to all the data—not simply names and addresses—held in lifestyle databases which have become common place in the last 5 years. There is the practical difficulty that once a name and address have been deleted they may be re-acquired from a new source and the cycle repeat itself. Erasure of all data other than name and address and blocking of the remaining data might be the better course, if the Directive permits the use of blocked data to flag those not to be mailed.

5.4.3 The right not to be subject to decisions solely based on automatic profiling or personality assessment is akin to a provision of French law. It is not clear what the practical effect of the provision would be. Where does the human element have to come in the decision making process? A balance needs to be struck between giving individuals reassurance that decisions about them are properly taken, and making available the benefits of systematic decision making tools.

5.4.4 Notwithstanding these uncertainties and practical difficulties, the general approach of the Directive to individual rights is to be welcomed. That is summarised by the right of an individual "to oppose, for legitimate reasons, the processing of personal data relating to him".

5.5 *Codes of Practice*

5.5.1 The UK Act requires the Registrar to encourage trade associations and similar bodies to produce codes of practice. These codes are to give guidance on how to comply with the Data Protection Principles set out in the Act. The Directive also contains a duty on Member States to encourage trade and professional bodies to produce codes. These codes are to be "on the basis of the principles set forth in this Directive". The Commission is given power by the Directive, having regard—amongst other things—to any such codes, to make regulations applying the Directive "to the specific characteristics of certain sectors". It is not clear whether these European Codes are intended—as with UK codes—to apply the rules laid down in the Directive or whether these codes are intended to replace the Directive. The latter would not be acceptable. General rules of data protection ought to be clear and binding on all. Codes should therefore apply the Directive and not replace it.

5.6 *Special Categories of Data*

5.6.1 Article 6 of Treaty 108 specifies certain data as specially sensitive and prohibits automatic processing of such data in the absence of appropriate safeguards. The categories are:

(a) criminal convictions;

(b) data revealing racial origin;

(c) data revealing political opinions or religious or other beliefs;

(d) personal data concerning health or sexual life.

To this list the Directive adds philosophical beliefs and trade union membership. It prohibits automatic processing of this data except with the consent of the data subject or under specific legal authority on important public interest grounds. Data concerning criminal convictions can only be held in public sector files.

5.6.2 At first sight it seems not unreasonable to suggest that there are particularly sensitive categories of data and that processing of such data should be specially protected. But, on reflection, three problems arise: first, data which is sensitive in one country might be a matter of indifference in another; secondly, apparently innocuous data can be processed for highly sensitive purposes; and thirdly, what is treated as a sensitive purpose in one place might be a matter of indifference in another and vice versa. Even in the absence of complete agreement on a list of sensitive purposes, it might be better not to extend the list of data but to look at a core of sensitive purposes.

5.6.3 A particular problem arises with criminal convictions. There is no prohibition in the UK on private sector bodies holding such information. There are restrictions imposed by the Rehabilitation of Offenders Act 1974 on the use of information about spent convictions. Nevertheless, the prohibition in the Directive looks too sweeping. May not a bank hold data about the criminal records of fraudsters? May not an employer with a car fleet note who of his employees has been banned from driving? May not a data user note which of his servants has been convicted of a data protection offence?

5.7 *Exemptions*

5.7.1 The UK Act includes a number of exemptions from the scope of the Act. The Directive has some exemptions which are not quite as extensive (eg. there are no exemptions for payroll, accounts and pension data, nor for simple mailing lists). The Directive has nothing comparable to the UK non-disclosure exemptions which permit disclosures to be made which have not been registered. The Directive seems to contemplate that disclosures are proper only if compatible with the purpose for which the data are held and there is no exception for the overriding interests of the community or third parties such as in order to save life.

5.7.2 Of great significance are the exemptions from subject access. The Directive allows information to be withheld from a data subject by a public authority in specified cases which largely correspond to the cases provided for in Treaty 108 and included in the UK Act. However, there is no provision, on the face of it, for subject access exemptions in the private sector generally and in neither sector can data be withheld to protect the data subject himself. Consequently, if a private organisation—eg. a bank—keeps information to identify potential fraud there is no possibility of keeping that from the data subject, and a doctor cannot—as he could under the UK Act and under Treaty 108—keep information from a patient to save that patient from serious harm. These seem to be significant defects in the Directive requiring further examination.

5.8 *Transborder Data Flows*

5.8.1 The Directive introduces new machinery for controlling transborder flows of personal data. The EC will form an area within which equivalent

protection of personal data is ensured by the Directive and so within which by Article 1 there are to be no restrictions on flows of personal data. Transfers of personal data either temporary or permanent to non-EC countries may only take place if an adequate level of protection is ensured (Article 24.1). Member countries must inform the Commission of cases in which there is not adequate protection. The Commission may negotiate with third party countries on behalf of the Community and may prescribe a list of countries which do ensure adequate protection. Member States may permit transfers in breach of Article 24.1 in particular cases, after informing the EC Commission and Member States and not having received notice of opposition within 10 days. In a disputed case, the Commission are to adopt unspecified appropriate measures.

5.8.2 It is not clear how this machinery is to work in practice. The Directive seems to suggest the advance licencing of transborder data flows, but it is doubtful whether either that or the 10-day dispute procedure is realistic in the context of, for example, international money transfer systems. Where a Member State informs the Commission of inadequate protection, it is uncertain how other Member States are to behave. A blacklist seems to be contemplated, but there is no mechanism for preparing it. It is not always self-evident that a country lacks an "adequate level of protection". The whole issue raises the contentious problem of extra territorial jurisdiction. These TBDF provisions have considerable implications for relations between the EC and both non-EC European countries and also between the EC and those countries which have accepted the OECD Guidelines on data protection, but which do not have private sector data protection legislation on European lines.

5.9 *Machinery*

5.9.1 The Directive requires Member States to have an independent supervisory authority with enforcement powers. The UK already has such an authority. The powers of the authority might be made somewhat wider by the Directive in that it would expressly have the function of monitoring the application of the Directive and would seem to have a general right of access to files.

5.9.2 Two Advisory Committees are proposed both chaired by EC Commission representatives. One consists of representatives of Data protection Commissioners and the other of Member States. The work of the Committees is in the hands of the Chairmen. Would Data Protection Commissioners see this as a proper machinery for expressing an independent view? The relationship and work of the two committees is not properly explained, but they are clearly only advisory. It would be unfortunate if this machinery simply legitimised the very extensive rule-making power in Article 29 which might enable the EC Commission to modify the application of the Directive in ways which might otherwise be unacceptable.

6. CONCLUSION

6.1 The Registrar welcomes the declaration in the Directive that it is to ensure the protection of privacy of individuals. By comparison the UK Act simply declares that it is to regulate the processing of data.

6.2 The Directive sets down rules for the lawfulness of data processing in the public and private sectors; it gives specific rights to individuals followed by general rules for good practice in data handling including specially sensitive data. The effect should to increase the protection of individuals in the UK. The Registrar welcomes this.

6.3 There do seem to be some points in the draft which could cause practical difficulties and which the Registrar hopes can be ironed out in discussions, for example:

6.3.1 Manual records are included quite comprehensively. Perhaps it would be better to use a selective approach concentrating on the particular records that cause concern.

6.3.2 Notification to the national supervisory authority is similar to the present UK registration system. The Registrar had hoped to concentrate registration on sensitive users.

6.3.3 The lack of exemptions from subject access in the private sector could cause problems—for example in the case of financial services organisations trying to detect fraud. The lack of exemptions permitting emergency disclosures of data could be a problem if the information were urgently needed to prevent injury or damage to health as is allowed by the UK Data Protection Act.

6.3.4 The rules for regulating transborder data flows to non-EC countries may cause international difficulty. It is probably unrealistic to expect countries such as the USA, Canada and Australia to follow EC legislation precisely. Perhaps the solution lies in looking at particular data flows and the protection of that data in individual countries.

6.4 In the light of the detailed comments made, a revision of the draft directive (SYN 287) to contain fewer detailed prescriptions and allow greater flexibility in achieving its objective in each member state might be helpful.

6.5 Overall, the Registrar welcomes the attempt to give individuals within the EC a greater measure of privacy and protection for any information kept about them.

PAPER B—Prepared for the Home Office Consultation on the European Commission's Draft Directive on Data Protection, 18 February, 1991

1. Introduction

1.1 This paper gives the UK Data Protection Registrar's comments on the proposal of the Commission of the European Communities (CEC) for a general Directive on Data Protection (SYN 287). The paper is in 4 sections including this Introduction, together with an Annex.

1.2 *Section 2* is a brief background which states the main points from the earlier paper published by the Registrar (1).

1.3 *Section 3* gives the reasoning for restructuring the current Draft Directive in order to ease the problems of coping with the different legal traditions in Member States and with a rapidly developing, all pervasive technology.

1.4 *Section 4* presents the principal ideas for a remodelled Directive including the consideration of a number of main points arising from the present Draft Directive.

2. Background

2.1 At the end of November 1990, the UK Data Protection Registrar published a paper giving his initial reaction to the Draft European Community (EC) general or framework directive on data protection (SYN 287). He welcomed the Directive's declaration that it was to ensure the privacy of individuals and he took the view that the express rules for lawfulness of processing, the specific rights given to individuals and the general rules of good practice should increase the protection of individuals in the UK.

2.2 The Registrar saw some difficulties which he hoped would be overcome in discussions on the draft. The areas identified were;

2.2.1 The comprehensive inclusion of manual records;

2.2.2 The wide notification or registration system;

2.2.3 The lack of subject access exemptions in the private sector and the lack of non-disclosure exemptions generally; and

2.2.4 The arrangements for regulating transborder data flows.

2.3 The Registrar expressed the hope that the Draft Directive might be revised to contain fewer detailed prescriptions and allow greater flexibility to Member States in achieving the prescribed standards of data protection. He concluded by again welcoming the attempt to give individuals within the EC a greater measure of privacy and protection for any information kept about them.

3. The Registrar's Approach in Principle

3.1 This paper explains a general approach to a possible revision of the Draft General Directive. It builds on the welcome given to the Draft Directive

(1) Data Protection in the European Community. Initial views of the UK Data Protection Registrar (30 November 1990) (see Paper A in this Appendix).

by the Registrar in his first paper and suggests a route for resolving the practical difficulties which he identified.

3.2 The Registrar accepts that there is a legitimate argument for an EC directive in the field of data protection in order to ensure the proper functioning of the single internal market. If there is going to be a directive prohibiting Member States from preventing trans-border data flows, then it is to be expected that there will be conditions imposed about the minimum acceptable data protection regime within Member States. Some have suggested that this problem raises the issue of community competence. The Registrar has not sought to concern himself with this issue.

3.3 The CEC declares in the Explanatory Memorandum that "the exercise must not have the effect of reducing the level of protection already afforded in the Member States". This admirable objective leads naturally to the further objective that the Draft Directive should "provide a high level of protection". The Registrar strongly supports the commitment to data protection which this approach demonstrates. However, perhaps the Commission's anxiety to ensure that the Directive encompasses the detailed provisions of existing legislation in the Community has resulted in a draft which allows little scope for Member States to choose how they will meet the Directive's requirements.

3.4 The Registrar would prefer a more flexible approach which, whilst achieving the required high standard of protection, also tries to take account both of the practicalities of information handling and the distinctive legal traditions of Member States. As an example of that flexibility it might be helpful to consider the use of notification as proposed in Articles 7 and 11. The Registrar's approach to registration (notification) remains largely as set out in his 1989 Fifth Annual Report to Parliament. He favours a selective scheme concentrating on sensitive users and purposes. He recognises, however, that the objectives of registration—principally the partial satisfaction of Articles 5(b) and 8(a) of the 1981 Council of Europe Convention on Data Protection (Treaty 108)—can in some cases be achieved by other means. The Directive could helpfully provide a menu of options for achieving these ends assembled from the views and experience of Member States. The notification requirements would be one choice on the menu.

3.5 One advantage of the Directive is that, unlike the Council of Europe Convention (Treaty 108), there will be the mechanism of existing community law to ensure that the legislation that Member States pass does actually satisfy the directive. A rule-making power (such as that envisaged under Article 29) could overcome any divergences from the required high standard of protection that might arise between Member States. This power is of such importance that further consideration might need to be given to the mechanism for exercising it.

3.6 Turning to the structure of the Directive, the Registrar sees it as providing two sets of rules; one set consists of detailed regulations (such as the provisions of information under Articles 9 and 13); the other consists of the general quality of data rules which reflect Article 5 and the related provisions of Treaty 108. The Registrar believes that this dual approach can lead to some confusion and that a restructuring of the Directive could make matters clearer.

3.7 The proposed restructuring of the Directive would bring the present Article 16 forward before Chapters II and III. It would become the chief requirement of the Directive together with Article 14, which confers rights on individuals; the Directive would thereby become more readily comparable with Treaty 108 and the provisions to be found in Articles 5

and 8 of that Convention. This is the cornerstone of the Registrar's revised proposals.

3.8 This restructuring would emphasise the primacy of the quality of data principles. The detailed regulations could then be introduced as subordinate interpretations, options or guidance which would give a desirable degree of flexibility to Member States to implement the Directive. The rule-making powers in the Directive would be used to ensure that the approach adopted by each Member State properly met the Directive's requirements.

3.9 The Registrar would welcome discussion on a revised structure for the Directive which he believes would satisfy the objectives of the CEC, the proper protection of individuals and the desire of Member States both for flexibility in implementation and the minimum necessary legislative interference in commercial activity.

4. A Revised General Directive

4.1 *Introduction*

4.1.1 The Registrar proposes that it would be helpful to remodel the draft Directive so that the principal articles were closely akin to Chapter II of Treaty 108 (See Annex). There would also need to be provisions about the object, scope, definitions, the control of trans-border data flows and machinery for reconciling differences between Member States; the more detailed proposals of the present draft Directive could usefully be embodied in the revision as guidance to the interpretation of the principal articles or options for implementing those articles.

4.1.2 The structure could be illustrated diagramatically as shown in Table 2.

4.2 *Explanatory Notes to Table 2*

4.2.1 The Registrar would start from the same point as the CEC with a declaration that the Directive is to ensure the protection of the privacy of individuals. The definitions could usefully be amended to avoid using the file concept so that the Directive looked rather at the uses made of personal data.

4.2.2 The Directive seems to cover manual records comprehensively. This raises issues both of principle and practicality. The Registrar recognises the problems that can arise with manual records, but is concerned both to avoid any conflict with Article 10 of the European Convention on Human Rights (Treaty 5) and also to ensure that the regulation proposed can be implemented in an acceptable and reasonable manner. Perhaps the difficulties can be overcome by including in this Directive only those manual records which are incorporated into an automated system in such a way that the computer system indexes and points to the manual record. Consideration could then be given to some legal instrument regulating those particular classes of manual records where there is a demonstrable case for special protection for the privacy of individuals—medical, social work and education records might be good examples.

4.2.3 Many of the activities of not-for-profit bodies give rise to issues of data protection concern. The Registrar would prefer to see the general exclusion of these bodies reduced even though it is qualified by restricting the data, by requiring consent and by prohibiting communication.

4.2.4 The Registrar's view of the primacy of Article 16 has been set out earlier. The Article could usefully be modified to refer in paragraph 1(b) to 'legitimate purposes' thereby following the formula in Article 5 of Treaty 108.

Table 2: A Possible Restructuring of the Draft Directive

OBJECT	Protection of Personal Privacy No Restriction on flow of personal data between Member States	Article 1	EXPLANATORY NOTES
DEFINITIONS Article 2	SCOPE Article 3	LAW APPLICABLE Article 4	4.2.1 4.2.2 4.2.3
QUALITY OF DATA (Treaty 108 Article 5)		Article 16	4.2.4
RIGHTS OF INDIVIDUALS (Treaty 108 Article 8)		Article 14	4.2.5
SPECIAL CATEGORIES OF DATA (Treaty 108 Article 6)		Article 17	4.2.6
DATA SECURITY (Treaty 108 Article 7)		Article 18	
EXCEPTIONS (Treaty 108 Articles 3(2) & 9)		Articles 15 & 19	4.2.7 & 4.2.8
LIABILITY AND SANCTIONS		Chapter VII	
TRANSBORDER DATA FLOWS		Chapter VIII	4.2.9
SUPERVISORY AUTHORITIES		Chapter IX	4.2.10
RECONCILIATION MACHINERY		Chapter X	4.2.10
FINAL PROVISIONS		Articles 31, 32 & 33	
SCHEDULE OF INTERPRETATION			4.2.11
Lawfulness of Processing	—	Arts 5 & 8	4.2.12 & 4.2.13
Legitimacy of Purpose	—	Arts 5 & 8	
Compatibility of Use	—	Art 6	4.2.14
Notification	—	Arts 7 & 11	4.2.15
Alternatives to Notification		———	
Informing the Data Subject	—	Arts 9 & 10	4.2.16
Application of Quality of Data		———	
Automated Decision Making	—	Art 14(2)	4.2.17
Principles by Codes	—	Art 20	4.2.18
Provision of Information	—	Art 13	4.2.19
Informed Consent	—	Art 12	4.2.20

4.2.5 Similarly, Article 14 conferring rights on individuals ought to have a prominent position in the Directive. Article 14(2), reflecting Article 2 of the French Data Protection Law, might more appropriately be looked upon as a rule about how data should be processed and would, therefore, fit better in the proposed new schedule for the interpretation of the quality of data principles. The second sub-paragraph of Article 14(4) would sit more comfortably in Article 15 if the Registrar's view of that Article were adopted.

4.2.6 The attempt to specify classes of specially sensitive data runs into the difficulty that sensitivity is often determined by context. Rather than seek to specify a list of sensitive contexts or purposes, or, on the other hand, try to extend the list of sensitive data, it would seem better to restrict Article 17 to the list of cases in Article 6 of Treaty 108. In particular, provision must be made for the keeping of information about criminal convictions in the private sector so as to accommodate the needs of employers and others such as large financial institutions seeking to protect themselves against fraud.

4.2.7 Article 15 provides for proper exemptions from subject access in the public sector, but ought to be extended to follow Article 9 of Treaty 108 in order to provide for appropriate private sector exemptions. An extension to the scope of the article—also reflecting Treaty 108—could provide for exemptions from the restrictions on disclosure in cases where the information is urgently required to prevent injury or other damage to health.

4.2.8 The option given by Article 19 to Member States to make provision for the press and media might appropriately be included in the Exceptions section.

4.2.9 The trans-border flow arrangements are fundamental to the Directive and raise issues of concern. Clearly if the directive is to have any effect, one would expect to see some mechanism for guarding the data protection fence around the community. The proposed machinery requires member states to ensure that data transfers may take place only if the importing country ensures an adequate level of protection. By way of exception, this general rule may be waived in specific cases on proof of adequate protection in each individual case. That must result in either the complete black-listing of many countries or else suggests something akin to a case by case vetting of discrete data flows. That approach and the related appeals procedure with its ten day cooling-off period does not seem to reflect properly the practicalities of international data flows especially in the finance and travel sectors. Articles 24 and 25 could perhaps be remodelled giving each supervisory authority the power to prohibit transfers to countries with inadequate data protection, either generally or in specific cases. The CEC should retain the power to negotiate and publish a list of approved third countries. The machinery in Chapters IX and X should be used to reconcile any inconsistency of approach between the policies of national supervisory authorities.

4.2.10 The Registrar would stress the importance, in his view, of the Article 27 Working Party, which if it is to be properly independent ought to choose its own chairman. The significance of the rule-making power under Article 29 is dealt with at paragraph 3.5. Any rules should clearly be subordinate to, consistent with and in no way prejudicial to the general principles set out in the Directive.

4.2.11 The Registrar suggests that the most useful way of looking at a number of the Articles in the Directive is as guidance on the interpretation or implementation of the fundamental principles and rights set out in Articles

16 and 14. As they are subordinate to those general principles, it seems more helpful in understanding the shape of the Directive if they are placed in a Schedule at the end of the instrument.

4.2.12 Articles 5 and 8 set out some requirements for the lawfulness of processing in the public and private sectors. If detailed rules are to be specified, then they are likely to be different for the two sectors and therefore some distinguishing definitions will be required notwithstanding the problems those definitions create. The rules for lawfulness themselves create difficulties. First, it would be helpful if these rules followed the language of Article 5 of Treaty 108 distinguishing between lawfulness of processing and legitimacy of purpose. An appropriate modification should be made to Article 16.

4.2.13 The Registrar,secondly, would like to suggest a different approach to the content of Articles 5 and 8 which common law countries might find more comfortable and compatible with their legal traditions. Article 5(1)(a) could be a useful declaration about lawfulness of processing in the public sector, but perhaps there is no equivalent for the private sector. The remainder of Articles 5 and 8 could be seen as rules about the legitimacy of purposes for which data may be stored and would best be expressed as exclusions remaining silent about the total extent of legitimate purposes, but giving Member States the power to declare when a data subject has an overriding interest. As an example of this style of presentation, the following is a possible redraft of Article 8 (1) & (3):

"1. Personal data in the private sector shall not be treated as stored for a legitimate purpose if the data subject has an overriding interest except that in any event it shall be legitimate to store personal data for:

(1) a purpose to which the data subject has consented;

(2) the purpose of performing a contract or other legal duty for the discharge of which the personal data are necessary, or

(3) the purpose of correspondence where the data have come from sources generally accessible to the public.

2. Subject to sub-paragraphs 1, 2 and 3 thereof, Member States may specify the circumstances in which a data subject shall be treated as having an overriding interest for the purposes of paragraph 1 above."

4.2.14 Article 6 speaks of the communication of data where the purpose may not always be that of the public authority controlling the data. The Registrar's particular concern is that the current Article 6 permits too extensive disclosures of personal data by public authorities opening up the prospect of uncontrolled public-sector data matching. A proper application of the ultra vires principle would restrict the communication of data to those cases necessary for the performance of the functions of the communicating body. Article 6 can be seen as an interpretation of the requirement of Article 16(1)(b) that personal data should be used in a way compatible with the purposes for which they are stored and that their processing should be fair. A preferable form of drafting might be to specify those cases in which the use (which the Registrar takes to include 'communication' although that is expressly included in the definition of 'processing') or the processing are declared to be incompatible or unfair. The list of specified cases would clearly not correspond to the current Article 6. The remaining cases of communication would be judged on their merits by reference to Article 16(1)(b).

4.2.15 Articles 7 and 11 provide for notification to the supervisory authority. This system is comparable to registration in the UK except that under

the Directive notification is required if data are to be communicated. The Registrar would prefer a more selective system of registration comparable to that in the Irish legislation and concentrating on sensitive data users. Registration is a means of satisfying—in part at least—Articles 14(3) and 16(1)(b). It is a procedure which the Registrar supports in certain cases, but he would welcome other options being made available and set out in the Directive either explicitly or by giving Member States the opportunity to develop alternative solutions as suggested at paragraph 3.4 above.

4.2.16 Articles 9 and 10 are another means of satisfying Article 14(3) and perhaps also of specifying purposes as required by Article 16(1)(b). Articles 9 and 10 could therefore be seen as options to be considered with Article 11. Other options could be added for example, the provision of the Netherlands Data Protection Law which, subject to exceptions, requires controllers to notify data subjects on whom personal data have been recorded in a file for the first time.

4.2.17 Article 14(2) is drawn from French Data Protection Law. It is not entirely clear to those with limited experience of the application of the French Law how this enactment works in practice. It seems to the Registrar best viewed as rule about how data should be processed, but he retains some doubt about whether it should be an absolute rule. He would prefer it if the Directive required that in determining whether or not personal data had been processed fairly, regard should be had to—inter alia—whether an administrative or private decision involving an assessment of a data subject's conduct had as its sole basis the automatic processing of personal data defining his profile or personality.

4.2.18 Similarly, the duty to encourage the production of Codes of Conduct (perhaps better called Codes of Practice) should be placed in the context of the Quality of Data rules in Article 16. The Codes should be constructed to apply and implement the Article 16 principles.

4.2.19 Article 13 largely reflects the Registrar's standard advice on the fair obtaining of information in satisfaction of the duty imposed by Article 16(1)(a). There is a variety of cases and the Registrar would prefer it if that variety could be catered for by expressing Article 13 as considerations to which regard would have to be given in determining whether personal data had been collected fairly rather than as a strict rule to which there would be no exception.

4.2.20 The schedule might also contain provisions supplementary to the rights given to individuals by Article 14 and other provisions of the Directive. Article 12 with some slight drafting amendments would set out rules for a valid consent by a data subject. There may be other useful interpretative rules which could be added.

5. Summary and Conclusion

5.1 In summary, the Registrar welcomes a Directive which seeks to achieve a high level of personal data protection. He is, however, greatly concerned that the present draft does not adequately take account both of the practicalities of information handling and the distinctive legal traditions of Member States. The Registrar suggests that the same high level of protection could be achieved—in the field of automated data—by adopting a Directive which more closely followed the approach of Treaty 108. Articles 16 and 14 would set out the information handling standards to be achieved and the rights to given to individuals. Many of the other provisions could become options for the implementation of those

fundamental articles or matters to be taken into account when assessing whether the standard required by those articles had been achieved.

Extract from:
"TEXT OF THE COUNCIL OF EUROPE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA"

CHAPTER II—BASIC PRINCIPLES FOR DATA PROTECTION

ARTICLE 4

Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

ARTICLE 5

Quality of data

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

ARTICLE 6

Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

ARTICLE 7

Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

ARTICLE 8

Additional safeguards for the data subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

ARTICLE 9

Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

ARTICLE 10

Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

ARTICLE 11

Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possiblity for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

PAPER C—A Possible Revision of the Draft Directive, 30 May 1991

This revision follows from views put forward in Papers A and B. It restructures the Draft Directive in order to bring the fundamental statements of individual rights and data user obligations to the fore. It also introduces some modifications to the Draft Directive, for example, in the coverage of manual data and in the way in which the public and private sectors are treated. Finally, it is designed to give greater flexibility to Member States as to how they apply the directive in detail, subject to their achieving equivalent protection for individuals.

Proposal for a Council Directive concerning the Protection of Individuals in Relation to the Processing of Personal Data

THE COUNCIL OF THE EUROPEAN COMMUNITIES

Having regard to the Treaty establishing the European Economic Community, and in particular Articles 100a and 113 thereof.

Having regard to the proposal from the Commission

In cooperation with the European Parliament

Having regard to the opinion of the Economic and Social Committee

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Single European Act, include establishing an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognised in the constitutions and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms; – – –

(24) Whereas the adoption of additional measures for applying the principles set forth in this Directive calls for the conferment of rule-making powers on the Commission and the establishment of an Advisory Committee in accordance with the procedures laid down in Council Decision 87/373/EEC (1),

HAS ADOPTED THIS DIRECTIVE:

CHAPTER 1: GENERAL PROVISIONS

Article 1: Object of the Directive

1. Member States shall ensure, in accordance with this Directive, the protection of the privacy of individuals in relation to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons to do with the protection afforded under paragraph 1.

Article 2: Definitions

For the purpose of this Directive:

(a) "personal data" means any information relating to an identified or identifiable individual ("data subject"); and without prejudice to the foregoing an identifiable individual includes an individual who can be identified by reference to an identification number or another identifying particular; provided that data shall not be treated as personal data if they have been depersonalised.

(b) "depersonalise" means modify personal data in such a way that the information they contain can no longer be associated with a specific individual or an individual capable of being determined except at the price of an excessive effort in terms of staff, expenditure and time;

(c) "processing" means any of the following operations: the recording, storage or combination of data, their alteration, use, transmission, dissemination, retrieval, extraction, blocking or erasure;

(d) "data controller" means a natural or legal person, public authority, agency or other body competent under Community law or the national law of a Member State to decide, either alone or with others, what will be the purpose for which data are to be processed, which categories of personal data will be stored, which operations will be applied to them and which third parties may have access to them;

(e) "supervisory authority" means the independent public authority or other independent body designated by each Member State in accordance with Article 6 of this Directive;

(f) "public function" means a function exercised by a government body in a Member State or a function of a public administrative nature conferred on a natural or legal person by Community Law, or by a law or a measure taken pursuant to a law of a Member State; and

(g) 'use' includes communication, and 'communication' includes the disclosure of data to anyone, including servants or agents of the data controller, other than the data subject.

(h) 'European Convention on Human Rights' means the Convention for the Protection of Human Rights and Fundamental Freedoms which was opened for signature on 4 October 1950 and subsequently amended.

Article 3: Scope

1. Member States shall apply this Directive to personal data except where the activities for which the personal data are stored or used do not fall within the scope of Community law.

2. This Directive shall not apply to data held by an individual solely for personal purposes.

3. Member States shall apply this Directive to all personal data processed by automated means.

4. Member States shall, to the extent that they can do so consistently with the European Convention on Human Rights and particularly Article 8 thereof, apply this Directive to such personal data processed other than by automated means as:

(i) are contained in collections of personal data organised to facilitate access by reference to data subjects, and

(ii) are either indexed by automatically processed data or comprised of data to which Article 6 of this Directive applies.

Article 4: Law applicable

1. Each Member State shall apply this Directive to:

(a) persons processing personal data in its territory; and

(b) persons resident in its territory and through whom non-resident data controllers exercise control over the processing of personal data.

2. Each Member State shall apply mutatis mutandis Articles 5, 6, 7 and 12 of this Directive to a user consulting personal data located in a third country from a terminal located in the territory of a Member State.

3. Where personal data are moved temporarily from one Member State to another, the latter shall place no obstacle in the way and shall not require the completion of any formalities over and above those applicable in the Member State in which the data are normally located.

Chapter II: Basic Principles for Data Protection

Article 5: Principles

1. Member States shall provide that personal data shall be:

(a) collected and processed fairly and lawfully;

(b) stored for specified, explicit and legitimate purposes and not used in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

2. It shall be for the data controller to ensure that paragraph 1 is complied with.

Article 6: Special categories of data

Member States shall provide that data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, data concerning health or sexual life and data relating to criminal convictions, may be processed only

(i) with the express and written consent, freely given, of the data subject, or

(ii) subject to such other specific safeguards against abuse and unauthorised access as may be prescribed in accordance with the domestic law of the Member State.

Article 7: Data Security

1. Member States shall provide in their law that the data controller shall take appropriate technical and organisational measures to protect personal data against accidental or unauthorised destruction or accidental loss and against unauthorised access, modification or other processing. Such measures shall ensure an appropriate level of security having regard to the state of the art in this field, the cost of taking the measures, the nature of the data to be protected and the assessment of the potential risks. To that end, the data controller shall take into consideration any recommendations on data security and network interoperability formulated by the Commission in accordance with the procedure provided for in Article 20.

2. Methods guaranteeing adequate security shall be chosen for the transmission of personal data in a network.

3. In the event of on-line consultation, the hardware and software shall be designed in such a way that the consultation takes place within the limits of the authorisation granted by the data controller.

4. The obligations referred to in paragraphs 1, 2 and 3 shall also be incumbent on persons who exercise actual control over the operations relating to personal data.

5. Any person who in the course of his work has access to personal data shall not communicate it to third parties without the agreement of the data controller.

Article 8: Additional rights of data subjects

Member States shall grant a data subject the following rights:

1. To oppose, for legitimate reasons, the processing of personal data relating to him;

2. To know of the existence of personal data and to know the main purposes for which they are processed and the identity and habitual residence, headquarters or place of business of the data controller;

3. To obtain at reasonable intervals and without excessive delay or expense, confirmation of whether personal data relating to him are stored and communication to him of such data in an intelligible form;

4. To obtain, as the case may be, rectification, erasure or blocking of such data if they have been processed in violation of the provisions of this Directive;

5. To obtain, upon request and free of charge, the erasure or blocking of data relating to him held in files used for marketing purposes;

6. To obtain, in the event of the application of paragraph 4 and if the data have been communicated to third parties, notification to the latter of the rectification, erasure or blocking; and

7. To have a judicial remedy if the rights guaranteed in this Article are infringed.

Article 9: Implementation of the Directive

The Schedule to this Directive shall have effect for the implementation of this Directive by Member States.

CHAPTER III: EXCEPTIONS

Article 10: Exceptions from Articles 5, 6 and 8

1. Without prejudice to Article 11 of this Directive and paragraph 3 of this Article Member States may by statute except personal data from the application of Articles 5, 6 and 8 of this Directive:

(i) only for reasons relating to:

(a) national security

(b) defence

(c) criminal proceedings

(d) public safety

(e) a duly established paramount economic and financial interest of a Member State or of the European Communities

(f) the need for the public authorities to perform monitoring or inspection functions; or

(g) the protection of another individual, the data subject, or the rights and freedoms of others; and

(ii) in any case only to the extent that the exception is necessary in a democratic society.

2. In the circumstances referred to in paragraph 1, the supervisory authority shall be empowered to inspect the relevant personal data at the request of the data subject and the authority may, where appropriate, exercise the powers referred to in Article 17(2) of this Directive.

3. Member States may restrict the rights specified in Article 8(3), (4),(5) and (6) of this Directive in the application of that article to personal data used for statistics or for scientific research purposes provided that no data nor statistics nor the results of any research are published in a form which identifies any data subject and that no damage or distress is, or is likely to be caused, to any data subject.

Article 11

Member States may grant, in respect of the press and the audiovisual media, derogations from the provisions of this Directive in so far as they are necessary to reconcile the right to privacy with the rules governing freedom of information and of the press.

Chapter IV: Liability and Sanctions

Article 12: Liability

1. Member States shall provide in their law that any individual who suffers damage as a result of processing of his personal data or of any other act incompatible with this Directive shall be entitled to compensation from the data controller.

2. Member States may provide that the data controller shall not be liable for any damage resulting from the loss or destruction of data or from unauthorised access if he proves that he has taken appropriate measures to fulfil the requirements of Articles 7 and 13.

Article 13: Processing on behalf of the data controller

1. Member States shall provide in their law that the data controller must, where processing is carried out on his behalf, ensure that the necessary security and organisational measures are taken and choose a person or enterprise who provides sufficient guarantees in that respect.

2. Any person who collects or processes personal data on behalf of the data controller of the file shall in so far as it lies within his power fulfil the obligations provided for in Articles 5 and 7 of this Directive.

3. The person providing the service or his employees may divulge personal data collected or processed only with the agreement of the data controller.

Article 14: Sanctions

Each Member State shall make provision in its law for the application of dissuasive sanctions in order to ensure compliance with the measures taken pursuant to this Directive.

Chapter V: Transfer of Personal Data to Third Countries

Article 15: Principles

1. Member States shall provide in their law that the supervisory authority may prohibit the transfer to a third country, whether temporary or permanent, of personal data which would not receive an equivalent level of protection in that

country, provided that notwithstanding prohibition by the supervisory authority personal data may be transferred to a third country if the data subject has consented thereto.

2. Member States shall inform the Commission of cases in which an importing third country does not ensure an equivalent level of protection.

3. Where the Commission finds, either on the basis of information supplied by Member States or on the basis of other information, that a third country does not have an equivalent level of protection and that the resulting situation is likely to harm the interests of data subjects, it may enter into negotiations with a view to remedying the situation.

4. The Commission may decide, in accordance with the procedure laid down in Articles 20 and 21(2) of this Directive, that a third country ensures an equivalent level of protection by reason of the international commitments it has entered into or of its domestic law.

5. Measures taken pursuant to this Article shall be in keeping with the obligations incumbent on the Community by virtue of international agreements, both bilateral and multilateral, governing the protection of individuals in relation to the automatic processing of personal data.

Article 16: Opposition by Member States

1. A Member State may, in respect of a given export, a given class of personal data or a particular third country, give notice of opposition to the Commission objecting to the export of personal data from another Member State.

2. Where notice of opposition is given, the Commission may propose appropriate measures in accordance with the procedure laid down in Articles 20 and 21(2).

CHAPTER VI: SUPERVISORY AUTHORITIES AND WORKING PARTY ON THE PROTECTION OF PERSONAL DATA

Article 17: Supervisory Authority

1. Member States shall ensure that an independent competent authority supervises the protection of personal data. The authority shall monitor the application of the national measures taken pursuant to this Directive and perform all the functions that are entrusted to it by this Directive.

2. The authority shall have investigative powers and powers to secure compliance with the principles set out in and measures taken pursuant to this Directive. To that end, it shall have, inter alia, the right of access to personal data covered by this Directive and shall be given the power to gather all the information necessary for the performance of its supervisory duties.

3. Complaints in connection with the protection of individuals in relation to personal data may be lodged with the authority by any individual and the authority shall investigate and consider any such complaint if it appears to the authority to raise a matter of substance and to have been made without undue delay by a person directly affected.

Article 18: Working Party on the Protection of Personal Data

1. A Working Party on the Protection of Personal Data is hereby set up. An independent authority with advisory power, this Working Party shall be composed of representatives of the supervisory authorities provided for in Article 17, of each Member State, and a representative of the Commission. The Working Party shall elect a chairman for a term not exceeding five years.

2. The secretariat of the Working Party on the Protection of Personal Data, shall be provided by the Commission with the necessary means for the achievement of its task.

3. The Working Party on the Protection of Personal Data shall adopt its own rules of procedure.

4. The Working Party on the Protection of Personal Data shall examine questions placed on the agenda by its chairman, either on his own initiative or at the request of the Commission or a representative of the supervisory authorities, concerning the application of the provisions of Community law to the protection of personal data.

Article 19: Tasks of the Working Party on the Protection of Personal Data

1. The Working Party on the Protection of Personal Data shall:

(a) contribute to the uniform application of the national rules adopted pursuant to this Directive;

(b) give an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any draft additional or specific measures to be taken to safeguard the protection of privacy.

2. The Working Party on the Protection of Personal Data shall be consulted by the Commission on any proposed decision referred to in Article 15(4), any measure proposed to be adopted by the Commission under Article 16(2) and any measure proposed to be taken under Article 20 of this Directive.

3. If the Working Party on the Protection of Personal Data finds that significant divergences are arising between the laws or practices of the Member States in relation to the protection of personal data which might affect the equivalence of protection in the Community, it shall inform the Commission accordingly.

4. The Working Party on the Protection of Personal Data may formulate recommendations on any questions concerning the protection of individuals in relation to personal data in the Community. The recommendations shall be recorded in the minutes and may be transmitted to the Advisory Committee referred to in Article 21. The Commission shall inform the Working Party on the Protection of Personal Data of the action it has taken in response to the recommendations.

5. The Working Party on the Protection of Personal Data shall draw up an annual report on the situation regarding the protection of individuals in relation to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission.

Chapter VII: Rule-making Powers of the Commission

Article 20: Exercise of rule-making powers

The Commission may, in accordance with the procedure laid down in Article 21(2), adopt such technical measures as are necessary;

(i) to secure the implementation of the principles of this Directive in particular sectors having regard to the state of the art in this field and to any code of practice, and

(ii) to secure the uniform application of this Directive in Member States.

Article 21: Advisory Committee

1. The Commission shall be assisted by a committee of an advisory nature composed of the representatives of the Member States and chaired by a representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of any measure which the Commission proposes to take. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter, if necessary by taking a vote. The opinion shall be recorded in the minutes; in addition, each Member State shall have the right to ask to have its position recorded in the minutes. The Commission shall not implement a measure without the concurrence of the committee and failing such concurrence the Commission may refer any such measure to the Council who may deal with the measure in such manner as it thinks fit.

CHAPTER VIII: FINAL PROVISIONS

Article 22

1. (a) The Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 1 January 1993.

   (b) The provisions adopted pursuant to sub-paragraph (a) above shall make express reference to this Directive.

2. The Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field covered by this Directive.

Article 23

The Commission shall report to the Council and the European Parliament at regular intervals on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments.

Article 24

This Directive is addressed to the Member States.

Done at Brussels, For the Council

SCHEDULE

PART 1

1. (i) In the application of Article 5 (1)(b) of this Directive, Member States shall provide that personal data shall not be treated as stored or used for a legitimate purpose if the data subject has an overriding interest except that in any event it shall be legitimate to store or use personal data:

(a) to the extent that the storage or use are authorised or necessarily implied by Community Law or the law of a Member State;

(b) insofar as the storage or use are necessary for, or reasonably incidental to, the execution of a public function for which the data are stored or used;

(c) if the data subject consents to the storage and use;

(d) for the purpose of performing a contract or other legal duty for the discharge of which the personal data are reasonably required; or

(e) if the storage or use are required to prevent an imminent threat to public order, injury or other damage to the health of any person or a serious infringement of the rights of any person.

(ii) Subject to sub-paragraphs a, b, c, d and e thereof, Member States may specify the circumstances in which a data subject shall be treated as having an overriding interest for the purposes of paragraph (i) above.

PART 2

2. In the application of Articles 5(1)(b) and 8(2), Member States shall provide that the provisions of one or more of the following paragraphs shall apply namely:

(i) A data controller shall notify the storage and use of personal data falling within Article 6 of this Directive to the supervisory authority who shall record the information so notified in a register which shall be available for public inspection; the data controller shall notify any change in the purpose of the personal data and any change of address; and the information to be notified as aforesaid shall be specified by the Member States, but shall include the name and address of the data controller, a description in general terms of the relevant personal data falling within the said Article 6 and the main purposes for which they are stored or used; or

(ii) (a) A data controller shall notify every person on whom personal data have been stored for a specific purpose for the first time, within one month, that this has been done; such notification shall be given in writing and shall include the purpose of the file and the name and address of the controller;

(b) The requirement contained in sub-paragraph (ii)(a) above shall not apply:

1. if the data subject concerned is aware or can reasonably be expected to be aware that such storage has taken place;

2. if it is clearly in the interests of the data subject that no such written notification be given; or

3. if a request by the data subject to obtain personal data in pursuance of Article 8(3) of this Directive could be refused by the data controller; or

(iii) (a) When a data controller first communicates personal data or provides on-line access to that data he shall inform the data subject accordingly, indicating the purpose for which the data are stored, a description in general terms of the data and the name and address of the data controller;

(b) The requirement contained in sub-paragraph (iii)(a) above shall not apply in any of the circumstances mentioned in sub-paragraph (ii)(b) above nor if the communication is required by law.

3. Member States may allocate the application of the provisions specified in paragraph 2 above to different classes of personal data and they may vary the application of those provisions from time to time and may, after consulting the Commission, substitute therefor such alternative arrangements as will prove equally effective in ensuring that the principles set out in Article 5(1) and the rights granted by Article 8(2) are respected.

PART 3

4. Member States shall provide that, in determining whether personal data have been collected unfairly contrary to Article 5(1)(a) of this Directive, regard shall be had to inter alia whether an individual from whom personal data were collected had been informed about:

(a) the purpose for which the information was intended to be stored or used;

(b) the obligatory or voluntary nature of his reply to the questions to which answers are sought;

(c) the consequences if he failed to reply;

(d) the recipients of the information;

(e) the existence of the right of access to and rectification of the data relating to him; and

(f) the name and address of the data controller.

5. Member States shall provide that, in determining whether personal data have been processed unfairly contrary to Article 5(1)(a) of this Directive, in cases in which a data subject has been made the subject of an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality, it shall be for the data controller to show that the processing has no significant adverse effect on the interests of the data subject that warrant protection or to demonstrate that for some other substantial reason the processing is fair.

PART 4

6. (i) Member States shall provide that any consent within the meaning of this Directive given by a data subject to the processing or transfer of personal data shall be valid only if:

(a) the data subject has been supplied with the following information:

1. the purposes for which the data are to be stored used or transferred and the types of those data;

2. the recipients of the personal data;

3. the name and address of the data controller;

(b) the consent is specific and express and states the types of data, forms of processing and potential recipients covered by it.

(ii) Any consent referred to in paragraph 6(i) above may be withdrawn by the data subject at any time without retrospective effect.

PART 5

7. Member States shall provide that the supervisory authority shall, where it considers it appropriate so to do, encourage trade associations, professional

organisations or other bodies representing data controllers to prepare, and to disseminate to their members, Codes of Practice for guidance in complying with the principles set out in this Directive. Wherever practicable the preparation and dissemination of such codes should take place in collaboration with similar bodies elsewhere in the Community.

Appendix 2

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 8)

The research reported took place in February 1989, July 1990 and March 1991. 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 9 to 14)

The research reported took place in the first half of the years 1986, 1990 and 1991. Tables 13 and 14 only contain comparisons for the final two years.

The research method was to include questions in an omnibus survey conducted by telephone.There were 2,000 interviews with a representative sample of business establishments with less 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 British Telecom's business database.

Table 1

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

	Feb 1989	July 1990	March 1991
	%	%	%
Proportion saying the following are very important:			
Preventing crime on the streets	84	82	83
Improving standards of education	75	73	78
Protecting peoples' rights to personal privacy	72	70	73
Unemployment	68	58	70
Inflation	61	56	62
Protecting freedom of speech	61	51	58
Making sure women have equal rights	52	49	54
Protecting the rights of minority groups	33	27	35

Comments:

In general, views have remained fairly constant, although the perceived importance of unemployment, inflation, freedom of speech and the rights of minorities, after declining from 1989 to 1990, reverted in 1991 to the 1989 level.

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.

	Feb 1989	July 1990	March 1991
	%	%	%
Proportion saying the following are of most concern:			
Keeping personal information/details private	76	72	74
Protecting the privacy of my own home/property	74	72	74
Being able to do what I want in my own home	63	59	63
People telling me what to do/interfering in my life	57	55	57
Organisations building up files of information about me	54	54	51
Maintaining freedom of movement/speech/religion	53	50	51
Stopping unwanted mail/telephone calls/selling	52	56	56
Individuals prying into my business	49	49	52

Comment:

The privacy issues of most concern have stayed remarkably consistent.

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.

	Feb 1989	July 1990	March 1991
	%	%	%
Very concerned	39	43	40
Quite concerned	33	28	32
No opinion either way	9	8	8
Not very concerned	13	13	13
Not at all concerned	4	5	6

Comment:

In 1991, concern is greatest amongst 45-55 year olds (48% very concerned); those aware of the Data Protection Act (45% very concerned); and those aware of the Data Protection Registrar (45% very concerned.)

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.

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

Your Comment:

The level of concern has not fluctuated significantly other than with regard to information about earnings where, in 1991, fewer expressed 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.

	Feb 1989	July 1990	March 1991
	%	%	%
Doctors & the National Health Service			
Satisfied	90	88	91
Not satisfied	4	5	5
Banks & Building Societies			
Satisfied	83	80	83
Not satisfied	9	11	10
Employers			
Satisfied	72	71	75
Not satisfied	12	11	10
Police			
Satisfied	72	71	69
Not satisfied	18	14	20
Inland Revenue			
Satisfied	66	60	66
Not satisfied	19	19	19
Schools & Colleges			
Satisfied	61	61	65
Not satisfied	15	11	12
Departments of Health and Social Security			
Satisfied	59	58	61
Not satisfied	22	20	18
Shops & Stores			
Satisfied	31	33	35
Not satisfied	43	32	39
Credit Reference Agencies			
Satisfied	27	26	31
Not satisfied	47	44	44
Mail Order Companies			
Satisfied	25	21	23
Not satisfied	55	49	53

Comment:

There has been some increase in the last year in the number of people not satisifed with the police and not satisfied with shops and stores. Conversely, over the same period there has been some increase in the proportion reporting that they trust credit reference agencies and the Inland Revenue to keep and use information in a responsible way.

Table 6

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

	Feb 1989	July 1990	March 1991
	%	%	%
Proportion saying the following rights are very important:			
To correct errors in information about yourself	83	82	84
To know what the information about you is being used for	81	80	81
To be told who the information about you might be passed to	80	81	83
To be told where the information about you came from	79	78	78
To see information about yourself	75	75	79
To have yourself removed from the lists or files	70	64	75
To add things to the information about you	64	64	66

Comments:
The only significant change is that, over the last year, there has been an increase in the numbers of respondents who feel that it is very important to have their personal details removed from lists or files.

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.

	Feb 1989	July 1990	March 1991
	%	%	%
Aware there is a law concerning rights about information kept on individuals	18	18	22
Spontaneous awareness of the Data Protection Act	6	9	8
Prompted awareness of the Data Protection Act			
Definitely	16	18	18
Think so	9	12	11
Total Awareness of the Data Protection Act	31	38	37
Made use of the Data Protection Act	2	2	3
Think the Data Protection Act is very useful	61	60	66
Awareness of the Data Protection Registrar	23	35	36
Total Awareness of Data Protection*	42	53	53

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

Comments:
Awareness of the Data Protection Act and the Registrar increased after the television advertising campaign in 1990 and has held steady since. The increases,

over the last year, in awareness of a law concerning rights about information kept on individuals and in the number saying they think the Data Protection Act is very useful, are small but statistically significant.

Awareness is higher amongst: males (59%), 35–44 yr olds (66%), and amongst the AB (middle to senior management) (75%), and C1 (clerical and lower management) (68%) socio-economic groups.

Table 8

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

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

Comment:

There has been a steady, significant increase in prompted awareness of the right to see information and the right to correct information about oneself.

Table 9

Businesses were asked about their use of computers.

	Small Companies (less than 50 employees)			Large Companies (50 plus employees)		
	1986	1990	1991	1986	1990	1991
Sample size:	2026	1999	2001	357	398	396
	%	%	%	%	%	%
Type of Computer:						
Personal/Micro	18	24	27	84	77	89
Multi-user or mini computer	na	7	9	na	58	71
Word processor	9	14	20	73	69	81
Computer access terminal	9	6	8	77	44	49
Mainframe	na	1	5	na	42	36
Data processing carried out by outside body	8	5	6	na	19	25
Total with computer/ bureau use	31	40	45	100	98	100

Comment

There have been significant increases in the use of computers by small companies, especially personal computers and word processors. The use of computers is related to size: 27% of establishments with 1-2 employees having a computer, compared with 80% of establishments with 25-49 employees.

Table 10

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

	Small Companies (less than 50 employees)			Large Companies (50 plus employees)		
	1986	1990	1991	1986	1990	1991
Base: all who use computers	676	840	1036	357	391	393
	%	%	%	%	%	%
Hold personal records on computer:						
Yes	25	33	43	72	74	97
No	37	58	52	19	19	—
Don't know	39	9	4	9	6	3

Comment:

There has been a statistically significant rise in the proportion of both small and large companies that hold personal records on computer.

Table 11

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 (less than 50 employees)			Large Companies (50 plus employees)		
	1986	1990	1991	1986	1990	1991
Base: all who hold personal records	442	362	520	290	318	383
	%	%	%	%	%	%
Prompted awareness of the Data Protection Act	75	70	87	97	95	95
Semi-prompted awareness of the Data Protection Registrar	na	44	47	na	67	61

Comment:

Over the last year there has been a statistically significant increase in awareness of the Data Protection Act amongst small companies.

Table 12

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 (less than 50 employees)			Large Companies (50 plus employees)		
	1986	1990	1991	1986	1990	1991
Base: all with personal records	442	362	520	296	318	383
	%	%	%	%	%	%
Aware of the need to register	70	51	62	96	85	82
Awareness of data users obligations	na	26	26	na	47	44

Comment:

Over the last year there has been some improvement in small companies' awareness of the need to register under the Data Protection Act. Conversely, there has been some slipping away of knowledge of the need to register amongst large companies.

Table 13

Those businesses aware that there are other obligations imposed by the Act, aside from registration, were asked to list those obligations.

	Small Companies (less than 50 employees)		Large Companies (50 plus employees)	
	1990	1991	1990	1991
Base: all aware of data users obligations	104	148	147	149
	%	%	%	%
Provide individuals with a copy of the information held on them	50	36	53	48
Not disclose information to unauthorised persons	50	40	32	31
Ensure data is safe/secure	20	18	25	21
Make sure data is up to date	18	9	25	18
Hold data only for lawful purposes	12	4	11	13
Do not hold irrelevant or excessive data	10	1	6	6
Hold data no longer than necessary	10	3	4	3
Collect data fairly	6	3	5	10
Other	7	10	9	7
Don't Know	14	9	12	6

Comment:

Detailed knowledge of the Act's non-registration obligations (generally, the Data Protection Principles) amongst small companies has declined since last year.

Table 14

Questions were asked of those businesses holding personal records on computer to determine their awareness of rights given to individuals by the Act. Those aware that rights existed were asked to describe them.

	Small Companies (less than 50 employees)		Large Companies (50 plus employees)	
	1990	1991	1990	1991
Base: all who hold personal information	362	520	318	383
	%	%	%	%
Aware of individual rights	36	50	69	66
Base: all aware of individual rights	142	282	215	250
	%	%	%	%
Spontaneous understanding of individual rights:				
Individual's right to see what information is held on him or her	81	81	87	86
Right to correct information	18	7	22	8
Other	12	10	7	12
Don't know	7	7	6	4

Comment:

There has been a significant increase in general awareness of individuals' rights amongst small companies. However, there has been a significant decline in awareness, amongst both small and large companies, of individuals' rights to have inaccurate information corrected.

Appendix 3

Unaudited Financial Statement for the Year Ended 31 March 1991

STATEMENT OF RECEIPTS AND PAYMENTS FOR THE PERIOD 1 APRIL 1990 TO 31 MARCH 1991

	Notes	£	*1990/91* £	£	*1989/90* £
H. M. Grants received	2	3,152,796		2,970,599	
Operating receipts	3	1,944,366	5,097,162	5,264,502	8,235,101
Salaries and Wages		1,166,112		942,777	
Other operating payments	4	1,935,211	3,101,323	1,945,357	2,888,134
Surplus from operations			1,995,839		5,346,967
Other receipts	5	123,929		163,810	
Other payments	5	51,427	72,502	87,122	76,688
Surplus for Year			2,068,341		5,423,655
Appropriations	6		2,093,430		5,400,382
Excess of receipts over payments for the period			(25,089)		23,273

STATEMENT OF BALANCES AS AT 31 MARCH 1991

	Note	*1991* £	*1990* £
Balance at beginning of period		49,319	26,046
Add excess of receipts over payments for the period		(25,089)	23,273
	7	24,230	49,319

The following Notes form part of this Statement.

Notes to the Statement

		1990/91 £	1989/90 £
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 IX Vote 3 Subhead H3 1990-91	3,152,796	2,970,599
3.	Operating Receipts		
	Receipts from registration fees	1,944,366	5,264,502
4.	Other Operating Payments		
	Rents & Rates	224,601	132,552
	Maintenance, cleaning, heating & lighting	54,496	65,175
	Office supplies, printing, stationery	54,875	49,663
	Postage & telephones	53,460	50,994
	Travel & subsistence	113,051	77,469
	Staff recruitment	11,759	24,493
	Specialist assistance	31,229	17,416
	Public relations	493,958	629,915
	Legal costs	67,439	12,530
	Staff training/medical	28,186	29,400
	Computer bureau	588,551	634,667
	Vehicle expenses	1,571	976
	Audit fee	5,100	4,600
	VAT	206,935	206,507
		1,933,211	1,945,357
5.	Other Receipts/Payments		
	Receipts		
	Pension contributions/transfers	12,889	17,221
	Bank interest	107,396	111,760
	Speakers' fees	375	650
	Miscellaneous income		28,983
	Legal costs recovered	3,549	5,196
		123,929	163,810
	Payments		
	Purchase of computer hardware/software	22,460	37,054
	Purchase of furniture & other office equipment	22,302	38,703
	VAT	6,665	11,365
		51,427	87,122
6.	Appropriations		
	Amounts surrendered to the Consolidated Fund via the Home Office during the period		
	Registration fees	1,969,765	5,236,572
	Other	123,665	163,810
		2,093,430	5,400,382
7.	Balance at Period End		
	Cash at bank	23,950	49,053
	Cash held at offices	280	266
		24,230	49,319
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 504994 7/91 C15 3383/3 62359 G/N 155349 50401

HMSO publications are available from:

HMSO Publications Centre
(Mail 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)

HMSO Bookshops
49 High Holborn, London WC1V 6HB 071-873 0011 (Counter service only)
258 Broad Street, Birmingham B1 2HE 021-643 3740
Southey House, 33 Wine Street, Bristol BS1 2BQ (0272) 264306
921 Princess Street, Manchester M60 8AS 061-834 7201
80 Chichester Street, Belfast BT1 4JY (0232) 238451
71 Lothian Road, Edinburgh EH3 9AZ 031-228 4181

HMSO's Accredited Agents
(see Yellow Pages)

and through good booksellers

ISBN 0-10-255391-2

9 780102 553918