TENTH REPORT of the Data Protection Registrar June 1994

THE DATA PROTECTION REGISTRAR

LONDON : HMSO

TENTH REPORT

of the

Data Protection Registrar

June 1994

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

Ordered by the House of Commons *to be printed 5 July 1994*

LONDON: HMSO
£12.25 net

CONTENTS

Page 1 A PERSONAL NOTE

2 1. INTRODUCTION

3 2. THE UNITED KINGDOM IN THE EUROPEAN UNION
- (a) The European Union's Draft Directive on Data Protection
- (b) Other Relevant Directives
- (c) Police, Customs and Other Collaborative Initiatives
- (d) Collaboration between Data Protection Commissioners
- (e) Conclusions and Recommendations

7 3. ISSUES IN THE UNITED KINGDOM
- (a) National Identity Cards and Identity Numbers
- (b) The Confidentiality of Personal Financial Data
- (c) The Health Service
  - (i) The Confidentiality of Health Information
  - (ii) Ethnic Monitoring
  - (iii) The Mentally Ill
  - (iv) Genetic Screening
- (d) A Market in Personal Data
- (e) The Police and Criminal Justice System
  - (i) Retention Periods for Criminal Records
  - (ii) Converting Existing Criminal Records
  - (iii) Disclosure of Criminal Records
  - (iv) DNA Databases
  - (v) HIV/AIDS Markers on the Police National Computer
- (f) Open Government
- (g) The Child Support Agency
- (h) The Banking Industry
  - (i) The "Good Banking" Code of Practice
  - (ii) The Security of Banking Information
  - (iii) The Holding of Sensitive Personal Data by the Banks
- (i) The Insurance Industry
  - (i) The ABI Code of Practice
  - (ii) The Comprehensive Loss Underwriting Exchange
  - (iii) The Impaired Lives Register
- (j) Local Government and Schools
  - (i) Housing and Council Tax Benefits
  - (ii) The Local Government Review
  - (iii) Schools
- (k) An Abuse of the Data Protection Act – Enforced Subject Access
- (l) New Information Exchange Systems
  - (i) The Gone Away Information Network
  - (ii) The Council of Mortgage Lenders Anti-Fraud System
- (m) The British Code of Advertising Practice
- (n) Practices, Technologies and Techniques
  - (i) New Technology Forum
  - (ii) Calling Line Identification
  - (iii) Teleworking and Telecottaging
  - (iv) Geographic Information Systems

(v) Smart Cards
(vi) Data Matching
(vii) Document Image Processing
(viii) The Internet

31 4 DETERMINING THE MEANING OF THE LAW
(a) The Use of Customer Information by Regional Electricity Companies
(b) Innovations (Mail Order) Limited v. the Data Protection Registrar

34 5 COMPLAINTS FROM INDIVIDUALS

45 6 ENFORCING THE ACT
(a) Prosecutions
(b) Supervisory Actions
(c) Appeals to the Data Protection Tribunal
(d) Refusal of Applications to Register
(e) Monitoring compliance with the Act
(f) Use of a Warrant

50 7 THE DATA PROTECTION REGISTER

51 8 INFORMING PEOPLE ABOUT THE ACT
(a) Strategy
(b) Media Relations
(c) Publications and Educational Materials
(d) The Enquiry Service
(e) Conferences and Seminars
(f) Advertising
(g) Exhibitions

54 9 RESEARCH INTO ATTITUDES AND AWARENESS

55 10 INTERNATIONAL ACTIVITIES OUTSIDE THE EUROPEAN UNION

57 11 ORGANISATION AND FINANCE
(a) The House of Commons Committee of Public Accounts
(b) Grant-in-Aid
(c) "Open Government" and Office Resources
(d) Results for the year
(e) Recovery of Expenditure

60 12 CONCLUSIONS

APPENDICES

63 1 Personal Data held within the Finance Industry: Some Implications of the First Data Protection Principle with Regard to Confidentiality

69 2 Disclosure of Criminal Records for Employment Vetting Purposes – Consultation by the Home Office

74 3 Calling Line Identification (CLI), Caller Display – Use of Captured Data

77 4 Smart Cards – Report of the Information and Privacy Commissioner, Ontario, Canada

79 5 Research Results

87 6 Extract from the Summary and Conclusions of "Data Protection Controls and Safeguards". Report by the Comptroller and Auditor General, 20 August 1993.

88 7 Statement of Account for the Year Ended 31 March 1994

A Personal Note

Last year, I also started the Annual Report with a personal note. In it I recorded that I planned to retire at the end of 1993. Plainly that has not happened and a word of explanation is necessary.

The Home Office was unable to announce the name of my successor, Mrs Elizabeth France, until February. Mrs France's current responsibilities made it difficult for her to take up office before the middle of the year. The most appropriate date for a handover now seems to be the beginning of September. I shall, therefore, now retire from office on the 31st August.

It is not appropriate to repeat the acknowledgements I made last year, although I should like to give a final thank you to my staff for their friendship and support. However, the delay has given me the opportunity here to congratulate and welcome Elizabeth France. She inherits a very able, loyal and professional staff and I wish her and them every success in meeting the many difficult challenges which will lie ahead.

ERIC HOWE
June 1994

1 Introduction

This Report is for the year ending 31 May 1994, although in a few cases relevant actions taken since that date have also been included. For any readers who are not familiar with the Data Protection Act, the following description may be useful.

The Data Protection Act 1984 was the first piece of legislation in the United Kingdom to address the use of computers. It is concerned with information about individuals which is processed by computer (personal data). It introduces significant new rights for individuals to whom that information relates (data subjects). Such an individual generally has the right to:

— have a copy of the information about him or her which is held on computers;

— challenge the information if he or she believes it to be wrong and, where appropriate, have it corrected or erased;

— claim compensation for damage and any associated distress arising from the loss or unauthorised destruction or disclosure of personal data relating to him or her, or arising from the inaccuracy of such data.

The Act places obligations on those who control the contents and use of personal data on computers (data users). They must be open about that use through placing details of their activities on a Data Protection Register which is available for public inspection. They must also follow sound and proper practices. These practices are described in eight Data Protection Principles. Amongst other things, the Principles require that personal data should be obtained and processed fairly and lawfully, be accurate, relevant, not excessive and be kept secure. Computer bureaux have more limited obligations mainly concerned with maintaining appropriate security around personal data.

The Data Protection Registrar is appointed by Her Majesty by Letters Patent and reports directly to Parliament. The Registrar is charged with administering the Data Protection Act 1984 and supervising its operation. His or her decisions are subject to the supervision of the Courts and the Data Protection Tribunal, which is also established by the Act.

The Act is designed to allow the United Kingdom to ratify the Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data". This ratification took place on 1 December 1987.

2 The United Kingdom in the European Union

The United Kingdom's interest and involvement in data protection issues within the European Union continue to develop. In this Section I describe a number of activities which have data protection facets.

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

The draft directive now under consideration is a modified version of a proposal originally made in 1990 which gave rise to extensive comment. I published a detailed response to the modified proposal in last year's Annual Report. I also included a statement of a common position on the draft directive reached by the Data Protection Commissioners of the European Union. There appears to be a positive response to the Commissioners' views.

I ventured a guess last year that the directive would finally be in place late in 1994 with a new United Kingdom Data Protection Act in force around the end of 1996. Both those forecasts are proving optimistic. A guess of the end of 1995 and late 1997 for the respective dates would now seem more appropriate.

That is not to say that progress is not being made. Advances have been made by the Council of Ministers Working Party considering this issue under the Belgian and Greek presidencies. This Working Party is producing modified proposals. The Data Protection Commissioners will continue to seek a joint position on these modifications.

There are three aspects of the Revised Draft Directive which I would like to touch on in this report – the jurisdictional framework, the application to manually processed records and the regulation of transborder data flows.

As far as the jurisdictional framework is concerned, Article 4 requires each member state to apply the directive to "controllers" of data established within its territory or jurisdiction. So a United Kingdom company would be subject to United Kingdom law even in respect of any processing operations it has in other countries of the European Union. The converse is, of course also true. For example, an Italian company which collects and processes information on British people entirely in the United Kingdom would be subject, in respect of that activity, to Italian law through its parent located in Italy.

This approach is similar to that used in the regulation of organisations providing services, say in banking or insurance, in different countries of the European Union. Such regulation is based on the law of the member country in which the parent organisation resides.

* Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (COM(92) 422 final – SYN 287)

However, data protection legislation is about the protection of individuals rather than the regulation of industry. It is civil rights legislation rather than technical business legislation. The focus ought to be on ensuring that individuals can secure their rights readily and effectively with the support, through the use of enforcement powers if necessary, of their national data protection authority.

In common with some other Data Protection Commissioners, I am not persuaded that the proposed Article 4 gives proper protection to individuals. It does not seem right that Italian citizens, whose personal data is collected and processed entirely in Italy by a United Kingdom concern, should have to use United Kingdom law and seek redress in the United Kingdom if the terms of the directive are breached. The issue is one of practicality as well as ethics, for I find it difficult to see how my Office, or the United Kingdom courts for that matter, could, without some difficulty, ensure that decisions taken here were put into effect in another country.

From its very first version, the draft directive has applied to records which are processed manually. The revised version sought to narrow this approach somewhat without sacrificing the basic principle that such records merited protection.

I understand that there are differences of opinion amongst the Member States on this particular aspect of the draft directive. As disagreements will ultimately have to be resolved by qualified majority voting, the cover of the eventual directive may remain in doubt for some time.

The United Kingdom has opposed the inclusion of manually processed records within a data protection directive. However, in the light of the moves towards open government referred to in Section 3(f) it remains to be seen whether that opposition can be sustained.

Following considerable criticism, the rules governing transborder data flows have been changed significantly from the original draft. Transborder data flows may now be allowed to countries outside the European Union which do not provide an adequate level of data protection where:

— the data subject consents to the transfer in order to take steps preliminary to entering into a contract;

— the transfer is necessary for the performance of a contract and the data subject has been informed of the recipient country's inadequate level of protection;

— the transfer is necessary on important public interest grounds;

— the transfer is necessary in order to protect the vital interests of the data subject.

In addition, in determining whether an adequate level of protection exists in another country, regard may be had to matters such as the nature of the data and existing general and sectoral legislative provisions and professional rules.

Monitoring and appropriately regulating transborder data flows is clearly a very difficult task. And it will get worse. Increasing international collaboration and trading together with developments such as the Internet (see Section 3(n)) will ensure that this is the case. It is clearly neither practical, nor desirable for the European Union to build a wall around itself to protect its citizens from the misuse of data about them.

Because of this situation, I have recently heard the view that we should simply give up on the transborder data flow issue. I do not share that view. However, I do think that progress will only be made slowly and by targeting what seem potentially problem situations, studying these carefully and then taking whatever specifically directed action seems appropriate. It will not be for me to consider this approach further, but it may be one that my fellow Data Protection Commissioners could consider.

(b) Other Relevant Directives

It is not only the Draft Directive on Data Protection which raises data protection issues. There are two proposed telecommunications directives which also need to be considered. These are:

— Modified Proposal for a Directive of the European Parliament and the Council concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks. (COM(90) 314 Final SYN 288);

— Amended Proposal for a Council Directive on the application of open network provision (ONP) to voice telephony (COM(93) 182 final – SYN 437).

There are other relevant European Union activities also. Directives such as those regulating banking and insurance impinge on matters of data protection concern by prohibiting disclosures of personal data even to the data subject concerned. The Distance Selling Directive addresses areas of direct marketing which also raise data protection issues.

(c) Police, Customs and other Collaborative Initiatives

The increasing perception that crime no longer respects national boundaries is leading to closer co-operation between police forces and other bodies across the European Union. The different countries collaborating may currently have markedly different data protection regimes. Such co-operative ventures therefore require their own frameworks of data protection control.

Generally the approach is to build on the various national legislations. Through appropriate Conventions, national legislations will be reinforced where appropriate and mechanisms put in place to deal with possible conflicts. Each Convention is likely to need some form of data protection supervisory committee.

I have been consulted about the terms for two such Conventions – the proposed Customs Information System (CIS) and Europol, which is concerned with co-operation on intelligence matters by European Union police forces.

The headquarters for Europol has now been established in The Hague, and the Europol Drugs Unit (EDU) which falls under the Europol initiative is currently becoming operational. Work on a Convention for Europol has not progressed as quickly as the operational development. However, a Ministerial Agreement on the EDU prohibits the storage of personal data in a central collection. Ministers have also invited their national data protection authorities to supervise the activities of national liaison officers and, in particular, to check that the EDU's common database contains only non-personal data.

I welcome this Ministerial Agreement. My staff are discussing the necessary supervisory arrangements with the National Criminal Intelligence Service (NCIS) which is responsible for the United Kingdom role in the EDU. Staff have also visited the Europol headquarters along with representatives of other European Union Data Commissioners.

A further development is the European Information System (EIS) which is concerned with information on persons and objects of interest to the police and immigration authorities.

(d) Collaboration between Data Protection Commissioners

The Data Protection Commissioners of the European Union States with data protection legislation have met this year to consider the Draft Data Protection Directive. They have also had a meeting with the European Commissioner responsible for the draft directive and put their views directly to him.

The Data Commissioners have set up a number of joint working parties. One is concerned with the draft directive, another with European collaboration on policing, customs and related matters. A working group on telecommunications has met to consider the Draft Telecommunications Directive and the European Community Draft Directive on Open Network Provision to Voice Telephony. In addition this group is considering other European Union telecommunications legislation.

This kind of collaboration between Data Protection Commissioners of the European Union is growing and it will continue to grow. This is not only because of the various European Union directives and initiatives referred to earlier in this section, but also because of the desirability of seeking common solutions to shared problems. There will also be occasions where there is a need for collaboration on individual enforcement cases.

All this is creating increasing demands on staff time in each Commissioner's Office. Before long it may prove necessary to establish a secretariat function at European level to assist in administering collaborative work between the Commissioners.

(e) Conclusions and Recommendations

There is a grave danger that the European Union will finish up with a mixture of differing data protection regulations. In order to monitor the application and effectiveness of these regulations it appears that a series of similar advisory and administrative committees will be established. It must make good sense as well as good administrative practice and legal principle to try to introduce some rationalisation into this situation.

As far as legal principles are concerned, common solutions could be embodied in a primary legal instrument dealing with data protection matters. The Directive on Data Protection is the obvious candidate for this role. This directive could provide the data protection rules for other sectoral directives. If there were a clash with other directives, which even in the best ordered of worlds may occur, then the data protection directive should prevail. I strongly recommend this solution.

In administrative terms, the various collaborative initiatives for customs, police and immigration establish data protection rules and envisage control commissions to supervise those rules. It would now be helpful to consider whether the control commissions, which comprise the Data Protection Commissioners of the European Union, could be brought together and be supported by a common secretariat.

In 1989, I recommended to Parliament that the Data Protection Act 1984 should be changed. The objective was to improve the Act for individuals and simplify it, particularly in terms of registration, for data users. The Directive on Data Protection seems likely to bring many of the changes I recommended, but a revision of the Act is on hold until the directive is in force. If the directive is delayed any further, I would recommend that the Act should be simplified and strengthened in advance of, but so far as possible in anticipation of, the final directive.

3 Issues in the United Kingdom

I deal in this Section and in Section 4 with a number of the more significant data protection issues which are demanding attention. There are other policy matters being progressed in both the public and private sectors not listed here. Anybody interested in a particular sectoral matter not referred to here may obtain more information from my Office.

(a) National Identity Cards and Identity Numbers

I have commented in previous Annual Reports on national identification systems. In an appendix to my Fifth Report in June 1989 I included a discussion paper and news release on national identification systems. Many of the points made remain relevant and copies of this appendix are available from my Office.

Sometimes the comments in past Reports were of a general nature and sometimes they dealt more specifically with matters such as the use of the National Insurance Number or the new National Health Service Number. A discussion on national identification systems also took place when I appeared before the House of Commons Select Committee on Home Affairs on 24 October 1990. Discussion most often takes place about a national identity card, but it seems inevitable that a card and a national identity number will go together.

During the last year there have been a significant number of parliamentary questions to Ministers about policy in respect of a national identification system. These include requests for a national identity card and for studies as to the benefits of this. The Prime Minister has stated that there is a strong case to be made for identity cards but that there are practical difficulties in introducing them and other matters to be considered. He has indicated that the Government is looking at some of the options and proposed continuing to do so.

There are other developments outside Parliament. For example, the new money laundering legislation requires financial institutions to insist on proof of identity of customers. This seems likely to add to pressure for a common identification system. The Association of Chief Police Officers (ACPO) has been reported as dropping its opposition to the issue of a voluntary machine-readable national identity card.

Although the Government has stated that it has no current plans to introduce a national identification system, interest has clearly built up and the issue is a complex one. We could find ourselves in a position where a de facto national identification system has simply emerged.

We may all be required in practice to identify ourselves from time to time, although this may occur very infrequently. Many of us have means of identity whether they be passports, credit cards, employers' identity cards, or driving licences. When meeting an occasional request for identification, inevitably individuals will use these documents where convenient in a manner beyond their intended purpose. But this will generally be a matter of individual choice. It is not primarily through this mechanism that I see a de facto national identification system coming into being.

However, a de facto national identity card might conceivably develop if photographs are introduced on driving licences. With photographs on driving licences it seems inevitable that their attractiveness as a general means of identification will grow. Indeed, it is easy to envisage the introduction of arrangements, such as exist in some parts of the United States, for the issue of non-driving licences purely as a means of identification. Interest has already been expressed in Parliament in a dual purpose identity card and driving licence which would include, amongst other information, an individual's photograph, national insurance number and fingerprints.

A more restricted initiative, but one which might also give rise to a national identity card is concerned with social security benefits. The Secretary of State for Social Security is reported as saying that, over time, benefit books could be phased out in favour of a social security payment card. Those receiving such payments would produce this card at local post offices. It would be swiped through a machine reader and checked against a database.

As far as a national identity number is concerned, two nationally allocated numbers already exist; the National Insurance Number (NINO) and the National Health Service (NHS) Number. The NINO covers the adult population but a Child Reference Number has recently been established for child benefit purposes which becomes the NINO when the child reaches sixteen years of age. Thus the NINO effectively covers the whole population. The NHS Number also applies to the whole population.

Use of the NINO has already been extended into purposes other than that for which it was originally intended. It is, for example, used as the income tax reference number. In my Sixth Report in June 1990, I recorded the view that it was helpful that Ministers had decided not to use the NINO for the Student Loans Scheme. In my Seventh Report in 1991, I recorded that the Department of Social Security (DSS) had confirmed that, although there is no specific statutory restriction, the Department's policy was to restrict the use of the NINO to tax and benefit related purposes. At the same time, I reported the use of the NINO in connection with Personal Equity Plans (PEPs) and the Tax Exempt Special Savings Accounts (TESSA) Scheme. Following representations from the DSS, the Inland Revenue undertook to introduce a statement, in the PEP and TESSA Operator's Handbooks, that the NINO should not be used for any purpose other than validating applications with them.

However, towards the end of 1993, my Office was asked to comment on the Association of British Insurers (ABI) Northern Ireland Personal Injuries Claims Register. In this register, the NINO is used as an identifier to facilitate the matching of insurance files. When this use of the NINO was queried, it transpired that the DHSS in Northern Ireland had been consulted by the ABI and had approved this use of the number.

The National Insurance Number is thus becoming more widely used as an identifier in both the public and private sectors. Government policy towards this seems to be uncertain. At the least, in practice, the policy does not seem to prevent the National Insurance Number from moving towards becoming a de facto national identification number. A clear policy to restrict the use of the National Insurance Number, supported by appropriate statutory controls could stop this movement.

The NHS Number is primarily generated on the registration of a birth, the system being derived from the old war-time national identification system. Last year I reported that a decision had been taken to re-issue NHS Numbers. The Department of Health and the NHS Management Executive had made it clear that they shared my wish to ensure that the new number is securely held and used only for NHS purposes. They had stated that it would be possible to pursue unauthorised use of the new number on the grounds that the NHS numbering system will be Crown Copyright.

I have now taken legal advice which calls this view into question. The actual NHS numbering system might be capable of copyright protection, but copyright protection is

unlikely to apply to individual NHS Numbers. A third party that simply asks its customers or clients to supply their NHS Numbers and records these on computer for its own purposes is unlikely to be involved in any substantial reproduction of the numbering system itself. Such an activity is therefore unlikely to infringe Crown Copyright.

It does, therefore, appear that Crown Copyright will not be readily enforceable as a remedy to counter possible extraneous uses of the new NHS Number. Nor of course will Crown Copyright restrict other Crown Agencies outside those concerned with health. I remain of the view I expressed last year – that statutory control of access to and use of the new NHS Number is appropriate if a policy of restricting its use to NHS purposes is to be successful.

In short, it appears to me that none of these four publicly created identification systems – the proposed driving licence with a photograph; the proposed social security "swipe card"; the National Insurance Number; and the National Health Service Number – is adequately protected against forming the basis of a de facto national identification system. Nor do there seem to be plans to provide such protection. A de facto system could therefore develop with no proper analysis of the advantages and disadvantages of such a system, without effective debate in Parliament and without proper statutory controls.

National identity cards were last introduced into the United Kingdom at the beginning of the 1939-45 war for security purposes. The use of these cards was effectively stopped by the judgement in Willcock v. Muckle* in 1951. In his judgement on that case, Lord Goddard gave his view that:

> "... to demand a national registration identity card from all and sundry, for instance, from a lady who may leave her car outside a shop longer than she should, or some trivial matter of that sort, is wholly unreasonable."
>
> "Such action tends to make the people resentful of the acts of the police and inclines them to obstruct the police instead of to assist them."

Experience may demonstrate an excessive use of an identification system. In Sweden a Commission on Personal Identification Numbers was appointed in 1993. Its task was to suggest measures to limit the use of the National Identification Number. The Commission has produced a draft of an Act which would introduce significant limitations on the use and availability of this number. The Commission has also proposed that it should be a crime to improperly use another person's identity.

Experience with the United States Social Security Number and the Swedish Personal Identification Number indicates that such numbers must be kept very secure otherwise they are of no value to authenticate the person who quotes the number. There are examples of the fraudulent use of these numbers in both countries which can cause considerable difficulties for the person to whom the number really relates. These numbers, which are effectively publicly available, are only able to signify the existence of a unique person; they do not of themselves show that a person who quotes the number is the person to whom the number properly belongs.

It is interesting that two other countries with similar backgrounds to the United Kingdom have: on the one hand rejected a national identity card (Australia); and on the other hand moved to prevent the de facto creation of a widely available national identification number (Canada). In Canada, when announcing the decision to restrict the use of the Social Insurance Number (SIN), the former Treasury Board President stated:

> "Many Canadians feel threatened by the use of the Social Insurance Number as a universal identifier. This measure marks the first step by the

* Willcock v. Muckle, All England Law Reports, Vol. 2 July 1951.

> Government towards its commitment to cap unnecessary collection and use of SIN."

and continued:

> "By restricting the use of SIN the Government is providing an example for other levels of government and the private sector to follow."

No national identification system should in any event be introduced without adequate safeguards. These should clearly control who may demand production of an identity card; who may demand to know a national identity number; who may collect national identification details on an individual and for what purposes such information may be used. It is interesting that the European Draft Directive on Data Protection (see Section 2) requires Member States to determine the conditions under which a national identifier may be used.

If pressures continue for a national identification system then it would be helpful to have a full and informed debate on the nature of such a system. Experience elsewhere and previously in the United Kingdom will be relevant. There should be a careful evaluation of any benefits which might flow from such a system and weighing of these against the undoubted risks to privacy and personal freedom. The argument, which is sometimes produced, that the innocent have nothing to fear, may have emotional appeal, but adds little of substance to the debate.

Ultimately, it is for Ministers and Parliament to decide on these difficult issues. If the United Kingdom decides to adopt a national identification system, then let it be introduced with care having learned from experience and built in necessary restrictions and safeguards. In any event the issue is too fundamental for the United Kingdom to allow itself simply to slip into having a de facto national identification system.

(b) The Confidentiality of Personal Financial Data

In last year's Report I published my initial views on the lawful processing requirement of the First Data Protection Principle. Since then I have been examining how those views might apply to the processing of personal financial data. In particular, I have considered the situation where there is a duty of confidence relating to customers' affairs. To assist me in this, I have taken advice from counsel in banking law.

In January, I circulated some views to finance industry representative bodies, regulators in the finance industry and consumer groups. These views are reproduced in the paper in Appendix 1. This paper outlines my understanding of the way in which a duty of confidence affects the processing of personal data in the finance industry.

Based on this understanding, some of the finance industry's current and proposed practices could entail the unlawful processing of personal data. This is because organisations in the finance industry have a practice of disclosing, to each other, confidential financial information on their customers' accounts. The information is generally disclosed through credit reference agencies.

The information disclosed is generally about credit or loan accounts. The information may be either adverse (so-called "black data") where an account is in default, or positive (so-called "white data") where an account has been properly handled. Finance Houses have disclosed both types of data for several years. Increasingly, banks are seeking to disclose not only "black" but also "white" data.

In effect the paper argues that, if personal data held under a duty of confidence are to be disclosed there should be specific consent from the individuals concerned. There will be exceptions to this and, under current law, consent to disclosure may be made a

condition of contract. However, the paper suggests that once the European Union Directive on Unfair Terms in Consumer Contracts is incorporated into United Kingdom law such a condition may be unlawful.

I have invited comments on my views. I have also expressed a willingness to discuss the issues with the main industry representative bodies and I hope such discussions can be arranged. The main responses seem now to be to hand. The reaction of the industry itself has varied but generally only in its degree of hostility.

The finance industry has also reacted sharply to the fact that my paper took account of the possible effect of the European Union Directive referred to above. This Directive is likely to be a part of United Kingdom law around the end of 1994. Not to consider the Directive now seemed to me a more likely ground for criticism.

I have made it clear on many public platforms that I consider credit reference systems to be valuable. In a paper reproduced in my Fourth Annual Report in June 1988 I stated:

> "In trying to resolve debt problems, it is necessary to seek a balance between:
>
> — the welfare of those borrowers who may get into difficulties or may be led into difficulties;
>
> — the commercial interest of lenders to protect their businesses and provide a viable, efficient service;
>
> — the interests of the borrowers in having such a service;
>
> — the privacy and data protection rights of the mass of individuals who meet their credit commitments without problems."

The law of confidence has its effect on that balance.

It can be argued that those who do fail to repay loans should lose some of their right to confidentiality. I am not unsympathetic to that argument, even though the advice I have been given suggests, on the face of it, that confidentiality applies even in these circumstances. On the other hand, it can be argued that those who do service debts properly should have control over whether their financial affairs should be revealed to others. My legal advice suggests that the law of confidence supports this position.

It would of course be possible to pass legislation to alter the law relating to breach of confidence in this area. That is a matter for Ministers and Parliament, not for me. If consideration is to be given to such a step it might usefully be as part of a wider review of the way in which the finance industry collects and uses personal data. Such a review could consider different points of view on the way such activities are or should be regulated. The results could put procedures on a firm footing for the future. That might well be in everybody's interests.

However, we are dealing with the law as it now stands. The law of confidence is a developed area of law. The finance industry is large and powerful and well able to marshal its views of the law. I will consider the industry's response to my paper with care. If, at the end of the day, our views of the law and its effect differ, then this may be a matter for the courts to decide.

(c) The Health Service

In 1991 the Government introduced a programme of reform in the National Health Service (NHS). The reforms include the establishment of NHS Trusts, the introduction of general practitioner fundholders, the development of an internal market in healthcare

and the encouragement of closer working relationships between health authorities. The NHS reforms are supported by an information management and technology strategy. Components of the strategy include a new format NHS number, shared NHS Administrative Registers and a system of NHS–wide networking. It is important that all these developments have proper regard to the requirements of the Data Protection Act. It is also important that they do not compromise the standards of confidentiality required by personal health information.

(i) *The Confidentiality of Health Information*

The Department of Health (DoH) has, for some years, been promising guidance on the confidentiality of health information. Section 2(3) of the Data Protection Act 1984 gives an opportunity for the Secretary of State to modify or supplement the Data Protection Principles to provide additional safeguards in relation to health data. My understanding is that the Government does not have it in mind to provide such further safeguards as a result of its guidance on confidentiality.

An Inter Professional Working Group (IPWG) produced a draft Code on Confidentiality of Personal Health Information and I expressed support for this code in my Fifth Annual Report (1989). There have been a number of further relevant developments since then, for example, legislation on patients' right of access to medical records, the introduction of new technology and genetic screening techniques. In the light of these, and in the continued absence of the DoH guidance on confidentiality, the BMA Council has decided that a group should be established to review the IPWG Code. One of my Assistant Registrars has been invited to attend its meetings.

In developing its guidance the DoH has consulted my Office on the requirements of the First Data Protection Principle. I anticipate that the guidance will include a sample notification for patients. This will inform patients of how their data might be used and disclosed. The notification will be for use throughout the NHS, albeit adapted to suit local circumstances.

Discussions with the DoH have centred on the extent to which patients should be given an opportunity to "opt out" of those uses and disclosures that are not necessary for their health treatment. How far, for example should patients be able to choose whether information they provide for health care should also be used for various types of research?

I have discussed the issues with the Chief Medical Officer and await with interest the DoH guidance on this point. My understanding is that the DoH recognises that information provided by patients is governed by a duty of confidentiality. This duty, on the face of it, restricts the use of such information to that directed to the care and treatment of the patient. The Department has taken the view that implied consent is given to further uses of patient data.

There is clearly a difficulty in balancing three different public objectives – the confidentiality due to the patient; the need for efficient administration of the NHS; and the wider public good which might flow from medical research.

In view of the importance of this matter I have decided to take my own legal advice. I have asked leading counsel for a view on a solution which I feel offers a balance which might be viewed as appropriate by the public and gain the support of the courts.

(ii) *Ethnic Monitoring*

I have now been asked for my views on the holding of individuals' "ethnic group" as part of NHS data. This would be included as part of the contract

minimum data set, or alternatively, be held on the proposed NHS Administrative Registers or existing Family Health Services Authority Registers. Section 2(3) of the Data Protection Act defines "the racial origin of the data subject" as one of the sensitive items of personal data which may be made subject to additional safeguards.

There are links between ethnic grouping, health status and health needs. Health authorities have a role in assessing the health needs of the population for which they purchase health care and may therefore need information on the ethnicity of both patients and the population as a whole. However, I remain to be convinced that this necessarily requires the routine holding of ethnic group data on all patients. Census information now provides a detailed breakdown of the ethnic mix of the population as a whole. This can be supplemented by sample studies or there can be targeted collections of data to provide information on the take up of particular health services.

I understand that the Commission for Racial Equality is broadly supportive of ethnic monitoring by the NHS subject to safeguards. Arrangements are being made to discuss this issue with the Commission.

(iii) *The Mentally Ill*

In December 1993, the Secretary of State for Health announced a requirement for mental health service providers to establish supervision registers. These registers identify those people with a severe mental illness who may be a significant risk to themselves or to others. Plainly, such registers contain very sensitive information and NHS guidelines have been issued to those who will be responsible for them. I commented on the draft of these guidelines. My comments aimed to ensure that those who are included on a register are aware of their inclusion and the use to which information on the register might be put; that their rights of subject access are not compromised; that the information held on registers is relevant and not excessive; and that registers will be kept securely. I am pleased that these points are catered for in the guidelines.

(iv) *Genetic Screening*

The development of genetic screening techniques and their application to health care raises a number of ethical and data protection questions. These result in part from the extent to which genetic screening of an individual might produce unexpected findings, or might reveal information directly relevant to the health of another member of that individual's genetic line. For example, are there circumstances in which an individual should be told that a genetic test has, incidentally, revealed that he is not the biological father of his child? Or are there circumstances where even though the subject of a genetic test refuses to give consent, information revealed by the test is so important to the health of another member of the genetic line that it should nevertheless be disclosed?

The Nuffield Council on Bioethics has recently published a report on "Genetic Screening – Ethical Issues". Amongst the report's conclusions are that, whilst computer based genetic registers are subject to the Data Protection Act, additional safeguards are needed for such registers. These safeguards include the storage of information in a safe place and manner, restriction of access to those specifically responsible for the register and the removal of identifying information when data are used for research purposes.

One of the report's recommendations is that the Department of Health should consider effective arrangements for the preservation of confidentiality, particularly in relation to genetic registers and should issue the necessary guidance. I welcome this recommendation. As mentioned in (i) above the Data

Protection Act offers the opportunity for providing additional statutory safeguards for health data. This would seem to be another instance where the creation of such safeguards would be appropriate.

(d) A Market in Personal Data

Last year I expressed concern about the existence of a market in personal data. In particular, I drew attention to third parties' gaining of unauthorised access to such as an individual's bank accounts. I concluded that the Data Protection Act 1984 did not offer an effective way of tackling this problem and that there was a potential loophole in the law.

In September 1993 I provided a report to the Home Secretary on this matter. I suggested that Ministers and Parliament should consider criminal sanctions to deter third parties from gaining unauthorised access to personal data. I also suggested that a fuller examination of the market in personal data would be helpful before final decisions were made. The Home Secretary responded that he would give careful consideration to the matter, although he felt further enquiries were not necessary.

This whole issue initially came to the fore as a result of newspaper investigations showing that it was possible to obtain information about well known public figures. Those about whom personal information was obtained included government ministers and the head of the security service. The matter was brought to public attention again early in 1994 as a result of an advertising campaign by an investigations agency. The agency sent letters to Members of Parliament and Members of the House of Lords amongst others. The agency offered to supply, for a fee, details of personal telephone calls, mortgage repayments, bank balances and arrears on electricity and other bills. It indicated that more sensitive areas of intelligence were available on request.

The sales campaign by this agent may constitute a classic case of shooting oneself in the foot. In the event Earl Ferrers, Minister of State at the Home Office, announced the Government position in a House of Lords debate on 24 March 1994. He stated that "We have to make it clear beyond doubt that a person who obtains unauthorised access by deception to personal data is guilty of an offence. We shall be seeking the necessary legislative provision to make amendments to the law in that particular case".

I welcome this response by the Government and look forward to discussions on the new legislation. I recognise that there may be a need for a defence of public interest.

(e) The Police and Criminal Justice System

Besides the material here, other references are made to police activities in Sections 2 and 10.

(i) *Retention Periods for Criminal Records*

Last year I described the moves that had begun towards establishing a comprehensive National Criminal Records System on the Police National Computer (PNC2). This system is now to be known as PHOENIX and it will start to become established in the next few months.

Consideration of the new system reopened the issue of for how long criminal records should be retained and the circumstances in which they should be deleted. I have had an understanding with the Police Service on these matters for some years. This understanding is based on information reported earlier to Parliament.

Details of the understanding are currently set out in the Association of Chief Police Officers' (ACPO) Code of Practice for Police Computer Systems.

Following discussion with my Office, ACPO modified the proposals it had made for extending the periods for which criminal records would be retained on PHOENIX and it has now been possible to reach agreement on many points. However, the nature of PHOENIX itself has thrown up a difficulty which it has not yet proved possible to resolve. PHOENIX is not restricted to conviction records alone but may also contain names of those acquitted of crimes. Plainly careful consideration needs to be given to the holding of such information on what purports to be a criminal record system.

Discussion so far has revealed two circumstances where details of an acquittal may need to be retained for a period of time. These occur under section 6(3) of the Sexual Offences Act 1956 and Section 27(3) of the Theft Act 1968. In both cases, the need for retention of acquittal information arises in connection with offences where certain defences can only be used once. The question as to whether there may be other exceptional circumstances justifying some retention of acquittal information is complex and agreement has not yet been reached with ACPO on this. I am awaiting a revised proposal from ACPO, but am concerned about the length of time it is taking to resolve this issue.

My staff have been reviewing the current ACPO Code of Practice with the Police Service. It is intended to publish an agreed revised version as soon as the PHOENIX record retention issues have been concluded.

(ii) *Converting Existing Criminal Records*

In order for PHOENIX to fulfil its intended role as a comprehensive computerised collection of criminal convictions, it is necessary to convert the National Identification Bureau's existing manual records into a form where they can be entered into the new system. Last year I reported that, in view of the costs involved, it was possible that this conversion of records might be undertaken overseas. Should this happen the requirements of the Act would apply, as data would be controlled from within the United Kingdom and be intended to be used in the United Kingdom.

I understand that this is still a possibility, but at the time of writing this report no decision has been taken. I am continuing to monitor the situation and will follow up the Home Office's assurance that my advice will be sought if the contract is placed overseas.

(iii) *Disclosure of Criminal Records*

The Home Office has issued a consultation paper on the disclosure of Criminal Records for Employment Vetting Purposes. Such disclosures raise some difficult questions of public policy, in particular how to achieve the right balance between the rehabilitation of offenders and the protection of vulnerable persons and property.

I have previously given evidence on this subject to the Home Affairs Committee of the House of Commons. I remain of the view that there should be a careful determination of who should have access to criminal records and in what circumstances. There should also be arrangements to protect the individual about whom requests are made. The access arrangements should be under the control of an independent body which is not dominated by interested parties. My comments on the Home Office consultation paper as a whole are reproduced in Appendix 2.

(iv) *DNA Databases*

In my Seventh and Eighth Reports I commented on the issues raised by the holding of databases of DNA profiles by the police. At the time there were suggestions from both the Home Affairs Committee and the Metropolitan Police Commissioner for large scale databases of DNA profiles, for example for the whole male population of the United Kingdom. Discussions were also underway between my Office and the Metropolitan Police about the retention of actual DNA profiles obtained in the course of criminal investigations. Whilst the Police & Criminal Evidence Act 1984 had established specific rules for the retention and destruction of fingerprints, the same was not true of DNA data and the legal basis for the retention and destruction of such data was, at best, uncertain.

To my knowledge, there are no present plans to establish large scale DNA databases of the type foreseen by the Home Affairs Committee. However, the issues relating to data derived from samples taken in the course of routine criminal investigation remain. These were recognised in the report of the Royal Commission on Criminal Justice, published in July 1993, which recommended that there should be clear legislative provision for a more extensive storage of DNA samples or data.

The police had argued that there should be power to take non-intimate samples without consent from all those arrested for serious criminal offences. This was for the purpose of DNA analysis in order to assist in the identification and conviction of offenders. The police requested the power whether or not DNA evidence was relevant to the particular offence being investigated. The data from those persons subsequently convicted would be retained in a database so that in any subsequent investigation where DNA evidence is available (for example from scene of crime stains) that evidence could be checked against the data in the database.

The Royal Commission accepted this argument and recommended accordingly. The effect, in terms of the power of the police to take samples and retain data derived from them, would be to put DNA evidence on the same basis as fingerprint evidence. This is an approach which I have supported in the past.

In the Criminal Justice and Public Order Bill currently being debated in Parliament, the Government has put forward proposals for dealing with samples for DNA analysis. In essence, the intention is to implement the Royal Commission recommendations regarding the taking of samples and the retention of those samples and data derived from them. My Office was approached by the Home Office for advice on the drafting of the relevant clauses in the Bill and detailed discussions have taken place between my staff and officials of the Home Office and the Forensic Science Service.

There proved to be a difficulty in drafting the Bill which derived from the way DNA samples are processed and kept. DNA analysis will be carried out by a "gene sequencer" which processes samples automatically in batches of 32 and stores the resultant band patterns as a digital image on an optical disk. Any individual image may contain band patterns both of persons who have been convicted and persons who have not. Separating them so that some can be deleted is not only difficult technically, but is undesirable from the point of view of preserving the integrity of the forensic evidence. Thus the raw data which is generated directly from the analysis process may need to be held, even though the samples themselves may have been required to be destroyed.

In the current draft, the Bill contains provisions requiring certain DNA samples to be destroyed. These might be where they have been taken from a crime victim or from a person who is subsequently acquitted. To cater for the technical and integrity problems arising from the DNA processing, the Bill provides that data derived from such samples may not be used in evidence or for the investigation of

an offence. The data which is usable for these purposes will be copied out on to a separate database.

Although the legislation will not prescribe specific retention periods, my staff will be discussing with the Forensic Science Service the policy for weeding of DNA records.

(v) *HIV/AIDS Markers on the Police National Computer*

Last year, I reported that a Home Office Circular (113/92) had recommended the removal of markers on the Police National Computer (PNC) which indicated a person's HIV status. This Circular was based on guidance from the Government's Chief Medical Officer. It concluded that the best protection for police officers lay in the adoption of standard hygiene procedures whenever circumstances might bring them into contact with blood and body fluids. The practice of relying on markers in police records identifying those with HIV infection was not seen as being an adequate method of protection, for it might tend to undermine the adoption of more protective standard procedures. The Circular recommended that police officers should have education and training in the standard hygiene procedures before the markers were removed. The end of 1993 was set as a target date for the completion of this process.

Although I understand that there has been some delay in the issuing of central guidance on training, it is now 18 months since the Circular 113/92 was first issued. My staff have now contacted all Chief Police Officers to ascertain the progress towards deleting the markers in question. Most Chief Police Officers have now responded and it appears that a small number are continuing to retain such markers.

In the light of the Chief Medical Officer's views and the Circular it would appear that retention of these markers on computer may contravene the Fourth Data Protection Principle which requires that personal data shall be relevant and not excessive. I shall consider responses from Chief Officers with this in mind.

(f) Open Government

The White Paper on Open Government (Cmd. 2290) was published in July 1993. This set out a code for access to information held by central government and proposed certain new statutory rights. One of the statutory rights would give individuals the right of access, subject to exemptions, to manual records about them held by government.

It was proposed that this new right should be analogous to the right of subject access to computer-held records given by the Data Protection Act. Whereas the Code of Practice on Access to Government Information is to be enforced by the Parliamentary Commissioner for Administration (the Ombudsman), the White Paper envisaged that the new statutory right would be enforced by the Data Protection Registrar.

The Government has responded to consultation on the White Paper by confirming its view that a new statutory subject access right is appropriate because it is an area:

> "...where personal rights are involved and where access provision needs to be combined with proper safeguards against unwarranted disclosure to third parties."

I welcome the approach taken by the Government. It extends a data protection right to an extensive class of manual records.

The suggestion that the new subject access right should be administered by the

Registrar's Office is sensible. It would allow the use of much relevant expertise already gained in administering the similar right given under the Data Protection Act 1984.

I briefly mention this subject in relation to the inclusion of manual data under the European Union's Draft Directive on Data Protection (see Section 2(a). I also comment again in Section 11.

(g) The Child Support Agency

The Child Support Agency (CSA) came into existence in April 1993. It is an Executive Agency within the Department of Social Security charged with the responsibility for assessing and enforcing maintenance payments by parents in respect of their children. Its activities are governed by the Child Support Act 1991 and a number of detailed regulations made under that Act.

From late 1993 I began to receive a considerable number of enquiries and complaints about the activities of the CSA. The bulk of the 200 complaints received so far have concerned the disclosure of income information in maintenance assessment notifications. Other complaints have been about disclosures of information by employers, misidentification of individuals and whether some CSA literature misleads in its references to confidentiality. These latter complaints are not dealt with here.

Many of those approaching my Office believed that, under the Data Protection Act, no information could be disclosed without the permission of the concerned individual. This view is not correct and complainants have been advised of this. However, an examination of the situation suggested that the CSA was routinely disclosing more detailed financial information than it was expressly required to do by regulations made under the Child Support Act.

Regulation 10 of the Child Support (Maintenance Assessment Procedure) Regulations 1992 requires the CSA to notify "relevant persons" of maintenance assessments. In most cases the relevant persons will be the parent with care (usually the mother) and the absent parent (usually the father). Such notifications must include:

— the assessable income of a parent with care;

— the absent parent's assessable income and, where relevant, the protected income level.

It is therefore a requirement of the regulations that the assessable income of an absent parent is to be disclosed to the parent with care and vice versa.

The regulations provide that a protected income level calculation is made in respect of all absent parents being assessed. This is to ensure that they and their new households do not fall below a minimum disposable income level as a consequence of maintenance payments. Where this would be the case then maintenance contributions are abated accordingly. The protected income calculation takes into account the incomes of others in the absent parent's current household including any heterosexual partner.

Therefore, where a protected income level is disclosed as part of the maintenance assessment notification this may involve, indirectly at least, giving some indication of the income of the absent parent's new partner. Not unnaturally, many new partners of those being assessed were very aggrieved at having their personal financial information given to a third party with whom they had no direct relationship.

The regulations state that maintenance assessment notifications must include protected income "where relevant". It was, therefore, suggested to the CSA that the protected income level should only be disclosed in those cases where it actually resulted

in an abatement of the maintenance payable by the absent parent. It was difficult to see how the disclosure of the protected income level was relevant where this was not the case. I am pleased to say that this view was accepted and that the CSA has implemented the necessary system changes.

However, the assessment notifications provided by complainants showed that a considerable amount of detail, regarding the basis on which assessable income and protected income had been calculated, was routinely being disclosed. The CSA has informed me that it is advised that it has a legal duty to provide such detail on all notifications as a matter of natural justice. This is in order that the parties concerned can make an informed decision about whether to appeal against a particular assessment. I have questioned this view and I am currently taking my own legal advice on this matter.

(h) The Banking Industry

(i) *The "Good Banking" Code of Practice*

At the time of last year's Report, the Code of Banking Practice Review Committee was considering responses to its consultation on the first edition of the code. I had expressed three concerns to the Committee. Firstly, that some banks have made it a condition of trade that individuals give their express consent for information about them and their accounts to be passed to other organisations. Secondly, that the protection against disclosure of customer details for marketing purposes has been undermined by the fact that many banks employ "host mailing" techniques. Thirdly, that some banks and building societies disclose both "black" (where an account is in default) and "white" (where an account has been properly handled) information to credit reference agencies. It was difficult to see how the latter disclosures were permitted by the code or under the Tournier rules governing banking confidentiality.

Representatives of the Review Committee were kind enough to visit my Office in February 1994 to present the final draft of the revised code, which was published in May. The revised code goes some way towards meeting my concerns. For example, paragraph 10.1, which deals with the marketing of services, states that: "Banks and building societies will not make the provision of basic banking services conditional on customers giving such written consent (to the disclosure of names and addresses to other companies in the same group for marketing purposes)". Also, paragraph 8.3 sets out a procedure for the notification of proposed disclosures to credit reference agencies. This is an advance on the previous edition of the code, which simply did not address the issue at all.

However, the revised code does not go as far as I would have wished in constraining the use and disclosure of customer details. These are matters which are, of course, linked to the issue of the confidentiality of personal financial data discussed in Section 3(b).

(ii) *The Security of Banking Information*

Concern about the existence of a market in personal data (see Section 3(d)) was, to a large extent, based on the fact that third parties had gained unauthorised access to personal accounts held by banks. The Data Protection Act did not offer a viable way of dealing directly with this problem. However, the Act does require that data users, such as banks, maintain appropriate security around the personal data they hold. With this in mind, I approached the main banks to see what was being or might be done to seal any loopholes in security which might be exploited by third parties.

My staff have visited twelve banks to discuss the security of customer

information. These discussions gave an overview of the variety of security practices in place. I was pleased to learn that many of the banks had taken significant steps to tighten their systems and procedures to combat attempts by unauthorised persons to obtain customer information to which they are not entitled. However, I continue to receive complaints about such activities. The following extract from a complainant's letter serves to illustrate the problem:

> "Two days later, on the Thursday lunchtime, I received another call from a person who identified himself as the controller of the ... Bank Computer Centre, who said that there was possibly a problem with two cheques which I had paid in, by hand, the day before to my branch at ... . He said that there appeared to be a simple error somewhere on my account and would I please just go through the last few transactions that I had made with him. After three or four minutes chatting, I suddenly became suspicious that he might not be who he had said he was, and asked him for some details about where he worked. He told me that he was "The Manager" of the ... Bank PLC, based at ... , with his phone number as 228-1919, and his name was Williams. When the call finished, I telephoned his number, only to discover that it is 'unobtainable' and when I checked with BT, even the operator said that this number is non-existent. I immediately tried to telephone my Bank Manager, and told a Mr ... my story. Mr ... said that the bank did not have any such centre at ... , and could not explain how the caller could have known the precise details of the two cheques which I banked the day previous. He did say that he would make enquiries of his staff though, and ring me back. When he did call back, he informed me that there had been some enquiries made to a member of his staff that morning, and that certain information had been passed on to a third party, including details of the day before's bankings. I asked the why's and wherefore's to be told that the member of staff who had divulged the information, had done so in good faith, believing that the enquirer was a member of the Bank's staff at their ... Branch, and this person had apparently used the Bank's "secret" pass-code to establish their bona-fides, before making several enquiries about my personal account details, all of which were freely supplied by my branch staff member."

The disclosure of customer data over the telephone raises particular security problems. I understand that financial institutions wish to offer wider services to customers over the telephone and I believe that large numbers of customers desire such services. It is in both parties' interests to ensure that such services do not compromise the confidential relationship between an individual and those he or she entrusts with the administration of his or her financial transactions.

I hope, in the near future, to publish further guidance for financial organisations on the disclosure of customer information over the telephone. A draft of this has gone for comment to the British Bankers Association and other interested parties.

A number of important points are worth stating here. Where automated services are offered to customers, involving the disclosure of information over the telephone without any human intervention, these should only be available to customers who have requested them. Also, security systems designed to "identify" staff in other locations must be looked at carefully. A password which is widely known by staff, can all too easily be passed to an unauthorised person. Reliance on the password system will then lull staff into a false sense of security. The use of simple procedures such as the return telephone call to a known secure telephone, in addition to a password could make some current systems significantly more secure.

(iii) *The Holding of Sensitive Personal Data by Banks*

In July 1993 media interest was aroused by the Data Protection Register entries

of some banks. These indicated that some banks held information about the political opinions and religious beliefs of their customers. The media coverage gave the impression that some banks were compiling dossiers about their customers' political opinions and religious beliefs.

As a result of this interest I approached the leading banks to seek an explanation of the circumstances in which any sensitive data about customers were obtained, used or disclosed. I referred specifically to the types of data mentioned as sensitive in Section 2 of the Data Protection Act 1984, namely: racial origin; political opinions or religious or other beliefs; physical or mental health or sexual life; and criminal convictions.

A survey of these banks showed that almost all of them hold information relating to racial origin in respect of their own staff, for monitoring equal opportunities policies. No bank appears to solicit information as to political opinions or religious beliefs. However, several have stated that such information may be recorded in free text form when volunteered by customers and when it is felt by bank staff to be relevant. Health data may be held about staff or, when banks have insurance divisions, about insurance policy holders. In a minority of cases, information as to the past criminal convictions of customers may be held where banks consider this is necessary to defend against fraud.

I am grateful for the co-operation I have received from the banks in looking into this matter. In the light of the responses given, I do not propose to take any further action at this stage. Individuals who are concerned about the sort of data held about them by banks or indeed any other organisation, should use the right of subject access given by the Data Protection Act. This enables individuals to obtain a copy of the data held about them. A leaflet explaining how to exercise the right of subject access is available from my Office. The leaflet also explains how individuals may complain to my Office if they believe a breach of the Data Protection Act has occurred.

(i) The Insurance Industry

Insurance companies routinely handle a great deal of sensitive personal data about their customers. In recent years there have been a number of significant developments within the insurance industry. New products have come on to the market, there has been a more systematic use of direct marketing techniques and the sharing of non-competitive information between different companies has been extended.

Here I refer to the Association of British Insurers (ABI) Code of Practice, the Comprehensive Loss Underwriting Exchange (CLUE) and the Impaired Lives Register. New matters will also need attention and I particularly have in mind the effect of the law of confidence on the collection and use of personal data. I dealt with this subject in respect of the finance industry in Section 3(b), but it may also have significant implications for the insurance industry.

(i) *The ABI Code of Practice*

Under Section 36(4) of the Data Protection Act I have a duty to encourage trade associations to prepare and disseminate codes of practice for guidance in complying with the Data Protection Principles. I was pleased to have been involved this year with the completion of the ABI Code of Practice. This was published in December 1993. The code gives helpful advice to those in the insurance industry and I look forward to continuing contact and discussion with the ABI on the code as practical experience is gained of its operation.

(ii) *The Comprehensive Loss Underwriting Exchange*

The Comprehensive Loss Underwriting Exchange (CLUE) is a database system through which insurance companies will share insurance claim data. When an individual applies for insurance cover for his or her house and contents or motor vehicle, the insurance company approached, if a member of CLUE, will be able to know what past claims the applicant has made. CLUE will therefore contain a good deal of detail on a very large number of people, which will be used not only for fraud prevention but for underwriting purposes.

It would have been helpful if my Office had been approached at an earlier stage in the development of CLUE. Since becoming involved there have been extensive discussions with the ABI to ensure that CLUE conforms to the requirements of the Data Protection Principles. As a result, it has now been possible to agree appropriate wording for insurance proposal, claim and renewal forms. However, it has not been possible to agree with the ABI that claims data for the past three years should be loaded on to the system. My current view is that this would lead to a breach of the duty of confidence which insurers owe to claimants and should only be done with a claimant's express consent.

(iii) *The Impaired Lives Register*

The Impaired Lives Register is a centralised insurance register. It contains details of individuals who have been refused life insurance cover, or supplied with life insurance cover at an increased premium because of health reasons. The Register is run by the Association of British Insurers (ABI). Whilst life insurance companies supply information to the central database, it is recorded in such a way that only the subscribing company can identify the individual concerned. However, the coding of the information does allow a company which receives an insurance proposal to find out if another insurance company has "impaired life" information on the applicant.

There has been an issue over how the Data Protection Act applies to the Impaired Lives Register, bearing in mind the type of information on it. This comprises a shortened version of the name of an individual, the date of birth of the individual, the insurance company registering the details and the category of insurance policy. However, it is agreed that, in supplying information to the Register, the insurance company is using personal data for a purpose which is different to the principal one of life insurance administration. Applicants for life insurance need to be made aware of this, and for this reason the ABI has included a clause in its code of practice asking insurance companies to draw attention to the Register in life and permanent health proposal forms.

(j) Local Government and Schools

(i) *Housing and Council Tax Benefits*

A large number of individuals claim Housing and Council Tax Benefits. To do so they are required to provide very detailed and sometimes sensitive information including income, family circumstances and, in some cases, disability details. There have been complaints about the collection, use and disclosure of the resultant records by local authorities.

As a result of these complaints my staff have had very wide ranging and detailed discussions on this matter with the Local Authority Associations, the Department of Social Security, the Institute of Revenues, Rating and Valuation and other relevant bodies. Following this, my Office has published a guidance document entitled "Administration of Housing and Council Tax Benefits: Requirements of

the Data Protection Act". Arrangements have been made to distribute this guidance to all relevant local authorities. It provides practical and authoritative advice to those who administer Housing and Council Tax benefits. The advice will be used to resolve existing complaints and should minimise future complaints.

(ii) *The Local Government Review*

The Local Government Act 1992 established the Local Government Commission for England with the purpose of recommending changes to local authority structures and boundaries. The data protection implications of such changes are being discussed with the Department of the Environment. The Office is increasingly being called on to provide advice to individual authorities affected by the Review particularly with regard to transitional arrangements and new registration requirements.

A particular issue has arisen about the limitations on the powers of local authorities. It has been drawn to my attention that local authorities may wish to use information, obtained by virtue of their statutory responsibilities, to put their views and positions on the proposed new arrangements before those affected. In one case referred to my Office, the authority had used its records of the names and addresses of individuals who are in receipt of educational grants to send information on the proposed reorganisation. The authority sought to encourage students to support its campaign to be retained as a unitary authority on reorganisation. It suggested that if the recipient supported the campaign he or she might wish to write to the Local Government Commission, local MP or the local press.

Whilst clearly local authorities wish to provide information to residents and have powers to do so, those powers are not unlimited. There may be restrictions on the use of information obtained for specific statutory purposes. I have doubts, in this particular case, about whether this is a proper use of the information concerned and have taken legal advice which suggests that the authority may have exceeded its powers. I have raised my concerns with the authority involved and am currently awaiting a response. In the light of the response I will, if appropriate, take steps to ensure that the implications of this view are drawn to the attention of other local authorities.

(iii) *Schools*

The management of schools education continues to change. This is causing changes in the way in which schools must register under the Data Protection Act. I proposed an additional clause in the 1990 Education Act to avoid re-registration where the governing body of a local authority maintained school in England or Wales becomes a corporate rather than an unincorporated body. I am pleased that this proposal was accepted. There has, however, arisen an issue of the possibility of delegating data protection responsibilities to Head Teachers so as to reduce the registration requirements. This is a matter of law which my Office is discussing with the Department of Education.

There have so far been over 27,000 applications for registration from schools in England, Wales and Northern Ireland. In Scotland, schools are still generally covered by local authority registrations. Those Local Education Authority areas from which there have been few registrations have been followed up. Once the point of law referred to above has been resolved I will be taking further steps to identify where schools have failed to register and will consider whether criminal offences may have been committed.

(k) An Abuse of the Data Protection Act – Enforced Subject Access

I have commented previously about the practice of requiring individuals to exercise their rights of subject access to criminal records and to national insurance records. The latter can indicate any period spent in prison, including time spent on remand.

This practice, which has become known as 'enforced subject access', first came to notice as a result of some employers' adopting it as part of their employee selection procedures. I have called for the practice in general to be prohibited, if necessary by criminal sanction, as it is a clear abuse of a right conferred on individuals by Parliament. I have also recommended that there should be a clear determination as to who should have access to criminal records and under what circumstances. The Home Office has issued a consultation paper on 'Disclosure of Criminal Records for Employment Vetting Purposes' and I refer to this in Section 3(e).

The practice of using enforced subject access continues to increase. Figures provided by the National Identification Bureau show 11,500 subject access requests for information from the Police National Computer System (PNC) in the year to March 1994. The Department of Social Security has also reported over 12,500 requests for national insurance records over a similar period. Both sets of authorities believe that the vast bulk of these requests, perhaps in excess of 90%, result from enforced subject access.

Use of the practice has spread outside employment vetting into other activities such as insurance claims and immigration enquiries. Both the Australian and Canadian immigration authorities now appear to have adopted this practice. This appears to have arisen as a result of a cessation of a previous arrangement with the National identification Bureau, under which these countries, together with New Zealand and the United States of America, were allowed to do a form of direct vetting check on criminal records.

Without an effective sanction to deter enforced subject access it is clear that matters are going to get progressively worse. A European Union Directive on Data Protection may ultimately prohibit the practice, but as can be seen from Section 2 this solution is still some years away.

(l) New Information Exchange Systems

(i) *The Gone Away Information Network*

I was approached in late 1993 by the Consumer Credit Trade Association (CCTA) with proposals to establish a database to be known as the Gone Away Information Network (GAIN). This database would hold information on individuals who have changed address, not notified a new address and who have defaulted on loan repayments. The intention was to provide a mechanism for the exchange of information on such individuals between credit grantors, credit reference agencies and other organisations such as public utilities.

My staff have had useful discussions with representatives of the CCTA and have commented in detail on the draft rules for the scheme. A number of points which I raised have been clarified and some of my suggestions have been taken on board.

There do however remain some concerns, for example, over the categories of individual on whom information would be held and the extent of the information itself, verification procedures and retention periods. I am also concerned at the

suggestion that public utilities may contribute to the GAIN database, particularly in the light of the advice I have received on the use of customer information by the regional electricity companies (see section 4).

At the time of writing, a six month trial of GAIN is under way with a limited number of participants. The trial is also restricted to one category of "gone away", following concerns expressed by my Office and referred to above. Discussions are continuing with the CCTA and I hope that it will be possible before the end of the trial to resolve any outstanding issues.

(ii) *The Council of Mortgage Lenders Anti-Fraud System*

I have advised on data protection issues arising from the Council of Mortgage Lenders (CML) Anti Fraud System. This system aims to detect cases of possible mortgage fraud, particularly ones involving multiple applications and fraud rings. Mortgage application details from different mortgage lenders are pooled and compared to detect any anomalies. Once an anomaly is found, perhaps a telephone number appearing on one application as that of a vendor and on another as that of a solicitor or surveyor, the system alerts the lenders involved so that they can make further investigations.

A pilot project involving about half a dozen lenders proved successful in helping to detect fraud. The system is now fully operational and is run independently of the CML. It appears that the system may now be widened to include other types of applications, for instance ones for consumer credit. I also understand that other companies are hoping to bring similar systems to the market.

Systems such as that developed by CML may hold considerable amounts of personal data and share these between large numbers of data users. It is important that data protection requirements are taken fully into account. The new uses and disclosures of personal data initiated by these systems should be explained to those individuals making mortgage or other applications. The personal data held should be used strictly for the purpose of detection of possible fraud. It should not be assumed that fraud is intended or has taken place simply because the system finds an anomaly, but rather that this simply indicates a matter requiring further investigation. Data users must not refuse subject access requests for personal data from these systems unless providing relevant information in a particular case is likely to prejudice the prevention or detection of a crime or the apprehension or prosecution of an offender.

(m) The British Code of Advertising Practice

Since 1991, the British Code of Advertising Practice has incorporated rules for Direct Marketing including List and Database Management. The code is administered by the Advertising Standards Authority (ASA) and sets a standard for the fair obtaining of information for direct marketing. I have previously welcomed this standard which is supportive of the requirements of the Data Protection Act. In June 1993 the ASA's Committee of Advertising Practice announced a review of the Code and sought comments from my Office. I understand that the revised British Code of Advertising Practice may be published early in 1995.

Over the years since the Data Protection Act came into force, the direct marketing industry has made significant changes to meet the standards of practice the Act requires. And it has mounted helpful initiatives such as the Mailing Preference Service. The result has been that complaints to my Office about direct marketing have largely faded away.

I appreciate that there are those in the industry who do not support statutory regulation. However, even they would perhaps agree that the dire consequences which

were predicted for the industry as a result of statutory regulation have not come to pass. Rather, I believe that the public has become more comfortable with direct marketing as a result of the more open stance now adopted. That can only be to the industry's benefit.

(n) Practices, Technologies and Techniques

New developments are constantly taking place in computing and communications practices, technologies and techniques. They can have significant implications for the collection, use and disclosure of personal data. This section draws attention to a number of significant developments some of which, for example Calling Line Identification, Document Image Processing and the Internet, are more advanced than others.

(i) *New Technology Forum*

On 13th May the first meeting of a New Technology Forum was arranged by the Rank Xerox Research Centre Cambridge Laboratory and my Office. The objective was to facilitate discussion of the data protection and privacy implications of new and emerging technologies. It is hoped that the Forum can have a continuing life and provide a valuable means of communication on these matters between government, research and academic communities and my Office. Rank Xerox acted as host for the May meeting and I will host a further meeting in the autumn.

(ii) *Calling Line Identification*

Calling Line Identification (CLI) is a technique which, in its simplest form, allows a person receiving a telephone call to read, from a display on the receiving instrument, the telephone number from which the call has been made. British Telecommunications plc (BT), having carried out trials on CLI, is now expected to launch a full service. Mercury Communications Ltd and other telecommunications operators can also be expected to introduce their own services.

I have dealt with the data protection issues raised by CLI in some detail in my Eighth and Ninth Reports. I have taken the view that CLI services should give the person making a telephone call the opportunity, at no charge, to suppress the transmission of his or her telephone number. This suppression should be possible on a per call basis (call blocking), or by blocking all transmissions from a particular number (line blocking). I am pleased to learn that both BT and Mercury will make call blocking and line blocking available at no charge on their respective systems.

At the time of writing, BT had just launched a partial CLI service (Call Return) in Bristol. This service allows a recipient of a call, by telephoning a certain number, to obtain the number of the last call received. Unfortunately, the introduction of this service had some unforeseen consequences, in particular certain users were able to get a full CLI display. Callers were not made aware of this. BT has taken steps to correct the matter, but it is disappointing that this has happened. This problem having been met once, I would not expect it to occur again.

CLI does not only offer the opportunity for an organisation receiving a call to read the caller's number, but also the opportunity to capture it. This can be done automatically by a computer system. Once captured, a number can, of course be used for other purposes. In Appendix 3, I give a preliminary view of how the Data Protection Act might apply in these circumstances.

(iii) *Teleworking and Telecottaging*

Teleworking is a term coined to describe working at a distance from the source of work. Telecommunications facilities are central to this type of work. A particular form of teleworking may be carried out through telecottages. The Telecottage Association defines a telecottage as "a local centre that provides low cost access to information technology and communications." The concept originated in Scandinavia and has spread to the United Kingdom where it has been introduced in both rural and urban areas. Telecottages offer the opportunity for computer-based training and employment in isolated and disadvantaged areas.

There are around ninety telecottages scattered throughout England, Wales and Scotland. In addition to telecottages there are other similar bodies in existence in more urban locations such as the "electronic village halls" in Manchester. These kinds of facility seem to be developing quite rapidly.

I think it is too early to say exactly how telecottages will develop in the United Kingdom. Financial support has been given from a number of sources including the European Union, local authorities and charitable organisations. The transition to financial self-support may not prove easy.

Educating teleworkers in good data protection practices presents a challenge. On the other hand, the presence of telecottages offers an opportunity to disseminate appropriate training and educational material.

(iv) *Geographic Information Systems*

A geographic information system (GIS) is "a system for capturing, storing, checking, integrating, manipulating, analysing and displaying data which are spatially referenced to the Earth. This is normally considered to involve a spatially referenced computer database and appropriate applications software."*

Geographic information systems provide data users with a powerful tool which presents information in new and readily accessible forms. There have been reported use of these systems by local authorities, supermarkets, building societies, insurance companies,hospitals, government departments and the police.

In essence, geographic information systems use a geographic reference point as a common identifier for many different types of information. Some of these systems will contain personal data which fall within the scope of the Data Protection Act. It is therefore essential that users of such systems are aware of the potential applicability of the Act to their processing of data within these systems.

(v) *Smart Cards*

Smart cards are effectively small computers held on a plastic card the size of a normal credit card. Smart cards have data protection and privacy implications in respect of who shall have access to the personal data on them and who shall have the ability to read, add to or alter those data. The range of possible uses of smart cards is growing rapidly although many proposed applications in the United Kingdom have only reached the stage of small-scale trials.

Smart cards have many possible uses in both the public and private sectors. These include their use for payment purposes, perhaps with facilities which create an "electronic purse"; for the prevention of credit card fraud; and for holding of details of medical conditions and treatment.

---

* "Handling Geographic Information: Report to the Secretary of State for the Environment of the Committee of Enquiry into the Handling of Geographic Information" Chairman: Lord Chorley, London, HMSO, 1987, p.132.

The Information and Privacy Commissioner of the Province of Ontario, Canada, has considered the data protection and privacy issues which are raised by the use of smart cards. He has kindly agreed to the reproduction of his proposed privacy protection requirements in Appendix 4.

(vi) *Data Matching*

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

Last year I wrote of my intention to gain an understanding of data matching in government departments. I described the approach I had made to the Permanent Secretaries of the Home Office and the Department of Social Security together with the Chairman of the Board of Inland Revenue seeking their assistance for a pilot study of their departments. The objective of the pilot study and subsequent enquiries was to determine what, if any, data matching took place in government departments and how this was developed and operated. Preliminary discussions have taken place with the three departments concerned. Follow up work to progress the study has been delayed by resource constraints.

(vii) *Document Image Processing*

Document Image Processing (DIP) is a technology usually based on the use of optical disks to store digitised images of documents. Documents are fed into the system in a process similar to scanning on a fax machine. The original document is returned and an image "held" on the optical disk. The image can be retrieved on screen and a copy made.

My Office has for some time been examining the issues raised by document image processing systems with a view to giving guidance to data users. With a traditional computer system, information is entered and processed in discrete fields enabling standards such as adequacy, accuracy and relevance to be applied separately to each piece of information about each individual. However DIP systems work in a different way. Information can only be processed at the level of a complete document or at least a complete page of a document. There is no straightforward way of separating items of personal data which are held on the same page.

It may be difficult for a data user receiving correspondence containing some relevant information and some irrelevant information to hold only the relevant information if the correspondence is to be stored on a DIP system. When determining relevance, account must also be taken of the inability of a DIP user to control the content of information that is volunteered whether in correspondence or otherwise. Such information may need to be retained because the data user requires a true record of correspondence received or because the data subject will expect the data user to be aware of the information. On the other hand where the data user solicits information from the data subject, whether on a form or otherwise, the considerations are likely to be different.

There are clearly difficult practical problems. However, I hope to be in a position shortly to issue guidance on a framework within which users of document image processing systems can operate whilst still complying with the requirements of the Act.

(viii) *The Internet*

We are all familiar with global communications in one form or another – post, telephone, facsimile, data communications. The reason these systems work and we are able to communicate with each other is because they have common standards. In other words, the telephone in the USA can communicate with the telephone in the United Kingdom because the various signals, establishing connections and transferring voice representations, for example, are agreed between the telephone network operators in each country.

Many of us are also now familiar with more discrete and limited network arrangements. Perhaps, for example, an intra-company network connecting geographically dispersed sites, or a local area network in a single office building. The users of each of these networks can communicate with others in the same network but may not be able to communicate with other networks. This is because the standards of such as message format and data encoding vary from one to another.

The phenomenon that is the Internet allows the users of these various networks to break out of their bonds and communicate with each other. It does this by establishing a set of messaging standards which can be set up at simple terminals or in the various networks to facilitate the sending or receiving of information in a common form.

The Internet has grown out of networks initially used for defence purposes and later linking research establishments in the United States. The common standards and the allocation of addresses are now administered and monitored by the Internet Society. The Society carries out this function through the Internet Architecture Board which is a group of invited volunteers. Through this mechanism the widespread demand to exchange ideas and information has effectively resulted in an upstaging of the conventional international standards activity. Users of the Internet can communicate freely with other users worldwide using electronic mail and bulletin boards, can transfer data files readily and have access to immense information resources.

What is striking is the way in which this common system has come into existence and the speed with which its use, on a global basis, is increasing. Various reports suggest that the number of users of the Internet now exceeds twenty million. Forecasts suggest growth to between one hundred and two hundred million users over the next 3-4 years. Not only is the use of the Internet increasing, but those using it are now coming from the commercial as well as the academic community. This movement is being hastened by a growing number of service providers. Those offering, or planning to offer services are now reported to include BT, the BBC and AT&T amongst many others.

Does the growth of a universal communications system such as the Internet challenge the orthodox data protection approach? In some respects it does not. The use of such a network for transferring personal data is subject to the same legal constraints as the use of a private network or indeed any other means of data transfer. The responsibility for meeting data protection requirements, for example, for accurate and secure personal data, still rests with the transmitting data user.

The challenge arises more in the sheer scale of the network. Can transborder data flow be effectively regulated when so many millions of data users have a relatively simple method of exchanging personal data with other data users overseas? Can privacy safeguards be established and enforced? These are among the questions which data protection authorities need to confront. The Draft European Directive (see Section 2) in its approach to transborder data flows forces similar questions.

The Global Village has arrived and with it have come two particular data protection challenges: how to monitor and control, if necessary, transborder data flows; and how to ensure the security of transfers of personal data.

4 Determining the Meaning of the Law

The Registrar cannot make a final determination of the meaning of the Data Protection Act; that is the role of the Courts. He does have to make his own decisions as to his views of the meaning of the law in the circumstances before him. In carrying out this function I have tried firstly to arrive at the decision the courts would make, secondly to achieve consistency of view and thirdly to propagate the view arrived at.

In my last Annual Report I gave some guidance on the approach which I have taken to the meaning and application of the term lawful in the Data Protection Principles. The term appears in the First Principle which requires that the information to be contained in personal data shall be obtained and processed lawfully. It also occurs in the Second Principle which requires that personal data shall be held only for one or more specified and lawful purposes.

During this year a number of issues have arisen where lawfulness has been a particular consideration. They are:

— the sharing of financial information by financial institutions (see Section 3(b));

— the confidentiality of health information (see Section 3(c));

— the use of information about student grants by local authorities in respect of the local government review (see Section 3(j));

— the use of customer information by utility companies.

As can be seen, I have dealt with three of these issues elsewhere in this Report. Here I touch on the use of customer information by the Regional Electricity Companies.

(a) The Use of Customer Information by Regional Electricity Companies

There are 14 licensed Regional Electricity Companies (RECs) in England and Wales. They use and disclose (or may propose to use and disclose) information for a number of purposes. The question is whether the activities in hand or in mind are lawful. I have at this stage only considered the position of the electricity companies but the possibility is that similar issues apply to other utility companies and I will be considering those in due course.

Utility companies are in a unique position for a number of reasons. They have a very high response from customers who notify them as to their change of name and address. This contrasts with many other available records, for example electoral rolls which are only brought up to date every twelve months. In addition, utility companies have comprehensive customer lists as they service most of the population.

It has to be recognised also, that the position of the individual customer of a utility

company may be different from the position of the customer in most commercial transactions. In many cases RECs, for example, have no prior contact with a customer before learning that he or she requires a supply of electricity. The REC does not, therefore, give any of the usual notifications of the uses and disclosures of personal data before it obtains information from individuals. In addition customers have no real option as to whether to have electricity, or choice as to the company on which they depend for supply.

The Electricity Act 1989 puts the RECs in a special position in relation to information obtained in the course of their businesses. The Act restricts the use and disclosure of customer information by RECs. There is also the additional factor that the powers of the RECs may be restricted by the ultra vires rule. I referred to this in my last Annual Report. It is the rule of law that those organisations which have statutory powers are only able to do those things which Parliament has allowed them to do. In the case of the RECs there are limitations on their contractual freedom to deal with consumers and these are set out in the Electricity Act.

I have now had an opportunity to take advice as to the position of the RECs. It is my view that a number of the uses and disclosures of information, current and proposed, by the RECs involve contraventions of the restrictions in the Electricity Act. The issues raised are complex. There may also be implications for the activities or proposed activities of other utilities. I shall wish to consult with other regulatory bodies in the utilities field, but I anticipate that formal guidance will be issued on this matter later this year.

(b) Innovations (Mail Order) Limited v. the Data Protection Registrar

On the 29th of September 1993 the Data Protection Tribunal delivered its judgement in the above case. The case had been heard by the Tribunal between the 6th and 9th of September. It arose as a result of an appeal by Innovations (Mail Order) Limited (Innovations) against an Enforcement Notice served by the Registrar on the 9th of April 1992. The Notice related to the practices adopted by Innovations in obtaining information from customers and enquirers. The Tribunal upheld the Notice subject to a variation which I had proposed.

Innovations conducts a mail order business in the course of which it advertises its goods in various ways, including through catalogues, advertisements in the press and television and radio. Customers respond to these advertisements in writing or by telephone. It is also the business practice of Innovations to make lists of its customers' names and addresses available for rental by other companies and this is a substantial part of its business.

Whenever a customer orders goods from Innovations the order is acknowledged in writing. It was the practice of Innovations to include a statement on the back of the acknowledgement. This statement informed customers that Innovations rented out names and addresses. The statement also gave an address to which the customer could write if he or she did not wish to receive such mail. A similar notification was also provided inside the catalogue produced by the company.

It was agreed that, on some occasions, the customer would not learn of the company's practice of list rental until after he or she had provided personal information. As a result I took the view that Innovations was unfairly obtaining such information. The Enforcement Notice required Innovations to give a notification of its practice at the point of obtaining in all cases.

Innovations argued that it was not practicable to give a notification on all forms of media, in particular on short radio or television advertisements. It argued that it was

more realistic to give the notice after information had been obtained from the customer. Innovations also submitted that this would be clearer to the customer because at the time of ordering he or she would be more concerned with the choice of goods than whether Innovations would trade the name and address supplied. The company further argued that a notification on the telephone would increase the cost of calls to the customer and that a later notification could be more detailed.

The Tribunal was referred to the Council of Europe Recommendation R(85)20 on the Protection of Personal Data used for Direct Marketing, the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the European Union Draft Directive on Data Protection published in October 1992.

After hearing detailed evidence and argument the Tribunal ruled that it was not sufficient to provide a notification with the acknowledgement of order. The Tribunal considered that the words "fairly obtained" direct attention to the time of obtaining not to a later time. Also that individuals should be informed of the purposes for which the data will used if those are not obvious.

The Tribunal concluded that, in circumstances such as those of Innovations, the law requires that a warning must be given before information is obtained. The Tribunal also commented that where this was not possible, for example where a decision was made to use existing information for new purposes, then the data user would have to obtain the consent of the data subject.

The Tribunal did not accept that it was impracticable to provide a notification within any form of advertising currently available and was not prepared to exclude any media from its judgement.

The Tribunal's decision generally confirmed the advice I have been giving to data users about the fair obtaining requirement contained in the First Data Protection Principle. I have now issued further guidance on this point following the decision and this is available from my office.

5 Complaints from Individuals

During this year 2,889 complaints have been received. The following table shows how this number compares with complaints received over the previous two years.

Year	*Number of Complaints*
1991 – 1992	1747
1992 – 1993	4590
1993 – 1994	2889

The sharp rise in the number of complaints reported last year was due to a short television advertising campaign run in March 1993. Possibly because of this campaign general awareness of the Data Protection Act, amongst the public, has increased (see Section 9). This in turn may well have led to the average of 56 complaints being received per week during this year compared with an average of 33 per week before the campaign.

This increased complaints activity has caused considerable extra demands on staffing. These demands have primarily been met by transferring effort from other activities, in particular from policy and compliance work such as that outlined in Section 3. It has also been necessary to recruit and train additional staff to handle complaints.

It has always been the case that a proportion of complaints can be dealt with by providing standard information and advice to complainants. General complaints about the use of personal data for credit referencing purposes or direct marketing lend themselves to this approach. The data subject who has a suspicion that inaccurate personal data are being held might also fall into this category. The policy of seeking to define such standard responses to common complaints has continued and led to productivity gains which have helped to offset increased demands on staff time.

On the other hand other complaints do not lend themselves to this standardised approach. They require a full and detailed investigation. The percentage of complaints falling into this investigated category fluctuates but recently has been running at 59% of all complaints received. Of the complaints cases closed during the year, 33% were dealt with in under 3 months, 66% in under 6 months and 87% in under one year.

Some 78% of all complaints are about data users in the private sector. The majority raise concerns about data in the finance industry. Complaints about issues concerned with consumer credit still account for 31% of all those received. Many are disputes about the accuracy of the information which the credit reference agencies hold. They may arise where the individual's own efforts to resolve the problem have failed. The agencies hold the personal data in question, but in order to have the data amended individuals must take up their problem with the credit grantor. It is often the case that the credit grantor is no longer holding any personal data about the account which may no longer be active. Often it is difficult for the accuracy of the record to be verified.

Enforcement Notices served against the four main credit reference agencies (CCN Systems Ltd, Equifax Europe Ltd, Infolink Ltd and CDMS Ltd) took effect on 31 July 1993. The notices regulate the information which can be extracted by the credit reference agencies from their files and passed to a lending organisation when an individual applies for credit. Previous problems included the extraction of information not only about the credit applicant, but about third parties such as previous occupants of

the applicant's address and persons with similar names or addresses. The agencies have had to make significant changes to their systems and complaints are being monitored to see how the new arrangements are working.

In the public sector the greatest number of complaints have been received about the Child Support Agency. The vast majority of complaints have come from absent parents and in some cases from their new partners who are concerned that financial information about them is being passed to the parent with care. These issues are dealt with more fully in Section 3(g).

This year some 200 individuals have voiced their concerns about the security of their personal data. Unauthorised disclosures of personal data can cause much distress. Also, once the disclosure has been made it is often the case that the damage cannot be undone. The complaints can lead data users to undertake a thorough review of their security procedures and staff training.

Whilst the vast majority of complaints are successfully resolved by discussion and negotiation some have resulted in prosecutions.

Some particular examples of complaints follow:

Case 1

The complainant received a postcard from his health authority with details of an appointment for the immunisation of his child. He was concerned about the amount of information shown on the card which included: the child's name; date of birth; health authority identifier number; the vaccinations which the child was to receive; the time and date of the appointment; the name and address of the doctor to be attended; the practice number; the health authority number; and treatment centre code.

The Registrar's Office had previously expressed concern and given guidance on the use of postcards displaying personal information. The health authority explained that the postcards were actually produced for them by the county council but that the National Child Health System was being reprogrammed to print sealed envelopes containing the information. These would be introduced to replace postcards.

However, several months later the complainant received another vaccination appointment postcard. On approaching the health authority again it was explained that the introduction of envelopes had been delayed but had finally and recently been introduced for all vaccination appointments. In addition all staff had been informed that other appointment postcards must be posted in sealed envelopes.

Case 2

The complainant obtained copies of his credit reference files from a number of credit reference agencies after being refused a charge card. He found details of adverse information relating to his son who no longer lived with him.

The complainant and his son shared the same first name but had different middle names. However, the items of adverse information on the file each showed both of the son's initials and consequently it could be seen that this information related to the son and not the father.

One of the credit reference agencies had agreed to disassociate the information relating to the son from the complainant. Another credit reference agency had said that it was not possible to make such a disassociation between a son and father when they

both had the same first name. They had instead suggested adding a Notice of Correction to the file.

Following investigation, all the credit reference agencies agreed to make the disassociation between the complainant and his son. The complainant was advised to continue using both his first and middle names when applying for credit.

Case 3

The complainants had received mailings from an appeal committee requesting donations for a scanner. The mailings referred to the fact that the recipients had been treated recently at a local hospital and it appeared that their names and addresses had been made available to the appeal committee by the hospital.

It was pointed out to the health authority that, under the Data Protection Act, personal data must be processed "lawfully". The term "lawfully" applies not only to criminal law but also to civil law including, for example, common law duties such as confidentiality. When a patient provides information for the purpose of his or her treatment a duty of confidence arises.

The health authority decided that patient data would not be used for appeal purposes in the future.

Case 4

The complainant received a telephone call from her GP's receptionist asking her to attend the doctor's surgery to re-register her young daughter. It transpired that her daughter's records had been removed from the doctor's list by the Family Health Services Authority (FHSA) without the parents' request or consent. The complainant made enquiries of the FHSA and was told that the records were transferred because an employee in the FHSA had changed her daughter's address, with the result that the child was registered with another doctor within the same area.

The FHSA issued new written procedures to operators who access computer records for amendments. The procedures were designed to ensure that the correct records were accessed by operators before any amendments were made.

Case 5

The complainant discovered that her son had records at three different hospitals. One of the records related to a mental hospital. On making further searches there was an entry to indicate that the complainant's son had attended a mental hospital as an outpatient and there was a referral to a social worker. The complainant was concerned because her son had never attended the mental hospital or been referred to a social worker.

It appeared that the complainant's son had taken part in a survey. This had been conducted by a psychiatrist. Subsequently the son's details were recorded on the records of the mental hospital where the psychiatrist worked.

The health authority agreed to delete all inaccurate references to the complainant's son.

Case 6

The complainant was having difficulty in obtaining credit. She obtained copies of her credit reference file from the credit reference agencies and discovered that a County Court Judgement had been registered at her address in error. The County Court Judgement was in the name of the complainant's neighbours.

The complainant had written to the four agencies and asked them to alter their records. She sent extracts from the electoral roll to support her case. The agencies refused to alter the entries as they reflected a public record. They suggested that the complainant add a notice of correction to her file.

The Court was approached to discover the name of the plaintiff who had taken out the County Court Judgement. Subsequently it was found that the plaintiff was no longer in business. However, the attention of the Chief Clerk of the Court was drawn to the evidence of the electoral roll and it was agreed that the Judgement should be set aside.

The agencies then removed the entry from the complainant's file.

Case 7

The customer of a bank complained that the credit control section of the bank had telephoned his home and had spoken to his teenage daughter about a loan which he was alleged to have with the bank. When the customer queried the situation further it became clear that because of a misspelling of the surname, the customer's details had been confused with those of another individual with a very similar name. Nevertheless the individual concerned had to make distinct efforts to show that he was not the person responsible for the loan. The complainant was concerned that this should have occurred and that inaccurate information about him may have been passed to a credit reference agency.

The bank apologised to its customer and confirmed that the information lodged with a credit reference agency had been corrected. The mistake on the account had occurred when a request for a change of address had been received. The bank made clear that its procedures required that no discussion of account details should take place with any third party including family members. The employee concerned had since left the bank's employment. The bank's procedures with regard to change of address were reviewed.

Case 8

Following the rejection of an application for a chargecard for hotel services, a complainant made a subject access request to the company. He received a response including a copy of personal data and a set of explanatory notes which referred to another chargecard and not the one he had applied for. He was also unsure that he had received a copy of all of the personal data which was held about him since it did not include information which he had provided in the application.

The company explained that not all the information which had been required in the application had been computerised since the application had been rejected. It further explained that it administered several chargecards and that the wrong explanatory notes had been included by a clerical error. It was nevertheless sure that the complainant had received a copy of all of the personal data which were held about him.

The complainant then provided copies of correspondence he had received from the company and pointed out that there were contradictions between this correspondence and the data which had been supplied. These points were put to the company. Although

the company continued to believe that it had supplied all the personal data that it held, further checks were made. As a result of this, additional data were found and supplied not only to the complainant but to other individuals who had made subject access requests and whom the company identified as not having received this additional information.

The company reviewed its procedures in order to prevent a recurrence of the situation.

Case 9

The complainant had been employed by the company, about which he complained, for some years, but had left of his own accord some months earlier. The complainant was divorced and made regular payments to his former wife. He received a letter from his wife's solicitors which mentioned that at the time of leaving the company he had been paid salary arrears which amounted to a considerable sum. The complainant alleged that the Managing Director of the company had passed on details of these salary arrears to his ex-wife without his permission.

As a result of the investigation of this complaint it was discovered that the company was not registered under the Data Protection Act in respect of personnel/employee administration although it was holding personal data for that purpose. It was also established that an unregistered disclosure had been made by the Managing Director of the company concerning the complainant's salary arrears.

The company was prosecuted for holding data for a purpose for which it was not registered and for disclosing personal data to a person not described in its register entry. The Managing Director of the company was also prosecuted. The company and the Managing Director were both fined for each separate offence.

Case 10

The complainant was continuing to receive unsolicited mailings from a company despite his frequent requests for suppression. He advised that his many requests to this organisation, including those addressed to the Managing Director and the company's solicitor, had been ignored.

Following investigation of this complaint the company arranged for suppression of the complainant's details. In addition, the organisation which had supplied the complainant's name and address also arranged to delete the information it held about the complainant from its lists.

Case 11

The complainant received repeated demands for payment from a company in respect of a maintenance contract for some household equipment. The complainant said that he had never had any equipment from the company although negotiations regarding a purchase had reached an advanced stage.

The company corrected its records and apologised for the inconvenience caused.

Case 12

The complainant and his wife had the same initials. The complainant's wife took out a loan in 1989. During 1993 the complainant received phone calls about the loan. When his wife made enquiries she was told she could not be given information about the loan

because it was not in her name. Her husband was later told that the loan was issued to him.

The loan company explained that the title of his wife's account was inadvertently changed to 'Mr' when the details of her loan agreement were input and the system flagged a potential match with him at the same address since he had had an account with them. The operator confirmed the match, in error, and the complainant's wife's loan details were updated with the details of his previous loan. This error only came to light when the loan was nearing completion as a result of a telephone call from the complainant.

The database was corrected.

Case 13

The complainant had bought furniture on an "interest free" credit scheme. The agreement she signed involved her paying a deposit and the balance within ten months. Well within the ten month period she paid the balance by cheque which she sent to the finance company by recorded delivery. She said she wrote her account number and her name and address on the back of the cheque.

The finance company contacted the complainant some time afterwards to inform her that her standing order had not been paid. She went back to them with full details of her payment of the balance including photocopies of the back and front of her cheque which her Building Society had been able to trace; the cheque by this time also bore the finance company's receipt stamp showing it had been received within the ten month period. Notwithstanding this, the complainant received a copy of a County Court Judgement entered against her and an instalment payment book. The Judgement was subsequently set aside.

Some time later the complainant experienced difficulty when trying to get credit. It was found that although there was no longer an entry on the credit reference agency's files relating to the Judgement there were entries relating to the account showing it to be in default. This matter was put to the finance company.

The finance company said that the account number given on the back of the cheque was incorrect and the money had been put in a suspense account; this resulted in the action that ensued. However, when the account was corrected the department concerned had not advised the credit reference agency.

The agency's records were corrected.

Case 14

In 1990 the complainant was involved in a minor car accident and was fully insured at the time.

Some time later she received a court summons relating to the accident and was advised to forward it to her insurance company, which she did. She later discovered that a County Court Judgement was recorded on her credit reference file for the sum of £1,208.

The credit reference agencies were informed that the Judgement arose out of a motor insurance case. It was also pointed out that this particular Judgement was irrelevant to the question of the complainant's financial standing.

All the credit reference agencies confirmed that the Judgement had been suppressed in their files.

Case 15

The complainant obtained a copy of his credit reference file from a credit reference agency. This included a County Court Judgement. Although the Judgement was recorded in his name he insisted that it did not relate to a debt which he had incurred.

Upon further investigation, it was ascertained that the debt was in respect of non-payment of water charges when the complainant was only sixteen years old.

Although the water company records showed the complainant as the person to whom water charges accounts were addressed, they agreed that he was unlikely to be the person responsible for the payment of the account due to his age.

The Judgement was set aside.

Case 16

Two doctors (X and Y) dissolved their practice with a third (Z).

When Z left the practice he took with him a computer which contained data relating to all the patients in the former practice. He then used this information to contact those patients who were registered with X and Y.

It was discovered that, when the partnership was dissolved, patients were given the option of which doctor they wished to be registered with. Although a majority of patients opted for the new practice of X and Y, many subsequently changed their minds on being approached by Z.

It turned out that Z was not registered under the Data Protection Act 1984. He admitted that he had used the data relating to the patients of doctors X and Y but had deleted the details of all patients other than those that had registered with him within 3-4 months of the dissolving of the original practice.

Doctor Z was prosecuted for failing to register.

Case 17

The complainant went into her Building Society branch and, during the transaction she was making, noticed on the computer screen that her date of birth was recorded as a date in 1942. She was somewhat annoyed as her real date of birth was in 1952! When she asked where the information had come from, the member of staff agreed that the information had not been supplied by the customer, but stated that, "It had been dreamed up by someone".

The Building Society explained that from 1982 onwards it began to ask customers for their ages (but not their dates of birth) and because a number of customers objected to this practice, some branches took it upon themselves to estimate the customer's age to avoid causing offence. By 1988 the financial market place had become increasingly competitive and date of birth information was perceived as a valuable piece of marketing data, so the Society decided to collect dates of birth on all its new customers. At this time the Society decided to convert the age information it already held into 'assumed dates of birth' on its computerised customer records. The Society took the view that this information recorded the expressions of opinion of its staff as to the age and occupations of particular customers and that it was therefore entitled to hold this data.

It was pointed out that the Fifth Data Protection Principle requires personal data to be

accurate and where necessary up to date. The Act points out that, 'data are inaccurate... if incorrect or misleading as to any matter of fact'.

In the light of this the Society agreed to delete all 'assumed' dates of birth.

Case 18

Mrs P P Roberts (names and addresses have been changed from the real ones) received a statement of account from a catalogue mail order company which indicated that the company thought that she was one of their agents. There was no debt outstanding on the account and it was sent to an address which was almost identical to that of the complainant.

The catalogue mail order company looked into the matter and identified records for an agent, Mrs P Roberts (but not Mrs P P Roberts). Mrs 'Roberts the agent' had lived at an address in the same area as Mrs Roberts the complainant. However, over a period of time, six different changes to the address of 'Roberts the agent' had been made on the company database. In common with many organisations, the company simply recorded changes of address notified to it by its customers or agents. Nevertheless, these six minor changes to the address of 'Roberts the agent' culminated in an address that was almost identical to that of the complainant. In consequence mail intended for 'Roberts the agent' was sent to Mrs P P Roberts the complainant.

The catalogue mail order company changed its records back to show the original address of 'Roberts the agent' so that the complainant would no longer receive mailings. It then attempted to contact its agent Mrs P Roberts at her original address, but received no reply.

It was considered that the circumstances of this case must raise some suspicions. It is possible that the facts indicate actions by persons unknown preparatory to the possible commission of a fraud. Mrs P P Roberts was advised of the existence of the Credit Industry Fraud Avoidance Scheme (CIFAS) and told that she could, if she wished, have her details registered with the Scheme. This should ensure that anyone applying for credit in her name would be subject to stringent identity checks before credit was granted. She was given this advice as a precautionary measure.

Case 19

Ms Clarissa Mary Green (names and addresses have been changed from the real ones) received an undated letter from the Student Loans Company Limited in Glasgow, signed by the Default Manager. It read: 'Due to your failure to respond satisfactorily to earlier reminder letters, your account has been passed to this department for the collection of £119.58 arrears. If you ignore this letter, your account will be passed to our legal department for court action'. Ms Green replied immediately saying that she had never needed, applied for, nor received, a student loan. Her mother also wrote saying that no other person living at the address had ever had a student loan and that she and her daughter, Clarissa had been the only two people resident at the address for the last fourteen years.

The Student Loans Company Limited replied stating that wrong information had been supplied to it and that it had removed details of Clarissa Green from its records. Whilst accepting the Student Loans Company apology, Clarissa Green was concerned as to how information about her had been connected with a defaulted student loan.

The resulting investigation discovered that a Ms Christine Mary Green, who had defaulted on a student loan had moved away from her address without telling the Student Loans Company. The Company requested a tracing agency to search for a new address.

The agency reported that it was "pleased to inform you that your customer is now resident at...", giving the address of Ms Clarissa Mary Green. The Student Loans Company sent an arrears letter from its default department addressed to Ms Christine Mary Green at the address which had been supplied relating to Clarissa Mary Green.

When it was discovered that Clarissa Mary Green was not the Christine Mary Green who was being searched for, the agency was asked to confirm the address it had supplied. On further checking, the agency came up with an entirely different address for Christine Mary Green.

Case 20

The complainant became aware that information relating to a number of past convictions was held about him by the police. He disputed the information recorded, saying that these convictions related to offences which he had not committed.

It transpired that another individual had been using the same name as the complainant as an alias. When records relating to this individual's convictions had been passed to the National Identification Bureau (NIB) by the local force concerned, they had been listed under the alias, and not the real name of the offender. As such, they were added to the records of the complainant.

The information was held in manual form, not on computer. The records held on the Police National Computer were in fact accurate, as they only included the reference number of the manual file held. However, the NIB arranged for the list of convictions to be transferred from the complainant's record to that of the offender.

Case 21

A complaint was received from a vicar that an electrical products store was sending to his address offers of extended guarantees for various products. He had no knowledge of the individuals to whom these offers were addressed nor of the products which had been purchased. He had lived alone for some time at his address.

It transpired that addresses provided by customers, which were sometimes incomplete, were sent by the store to a third party. The function of the third party was to complete the addresses where necessary in order to improve the targeting of follow-up mailings.

Post codes were normally supplied to the third party by the store with a total of six digits. Where the first part of the code consisted of four digits this meant that the last part would be incomplete. The third party was requested to complete it and did this by looking for the first valid occurrence of the six digit number on the Post Office Address File. Unfortunately for the vicar, in his area this was his address. Since his house was identified by a name but had no street name or house number the computer software compared the other parts of the address, found an apparently perfect match and deemed the match between the two addresses to be good enough to assume that they were the same. As a result of the complaint the electrical shop changed the address information provided to the third party to include provision for a seventh digit in the post code.

Case 22

The complainant was moving house. He had taken the usual steps regarding the utilities including cancelling direct debits and having meters read. He duly paid the final account to one of the utilities.

Six weeks later he received a letter warning him that a summons for an amount outstanding would be issued if this was not paid within seven days. The complainant was upset about this and also wished for confirmation that his records were accurate.

It transpired that although a direct debit payment was credited to his account at the beginning of the month he moved, this was subsequently reclaimed by his bank as a result of the earlier cancellation of its mandate. It is not normal practice of the utility to inform a customer that the account has been redebited where the customer instigated the cancellation of the payment.

It was possible to explain to the complainant the chain of events which led up to a demand for an amount which he had not realised was outstanding and to reassure him that the data held regarding the account were accurate.

Case 23

The complainant's 13 year old daughter received a catalogue from a mail order company. In order to check what information had generated the despatch of the catalogue the complainant submitted a subject access request to the company with the full knowledge and signed authority of the daughter. No response to this request was received within 40 days.

The mail order company explained that it had been unable to trace receipt of the complainant's request. However, as a result of the complaint the company immediately provided the complainant with the information requested.

Case 24

The complainant was a disabled woman who would have greatly benefited from the convenience of mail order shopping. However, she was denied the necessary credit facilities due to the close similarity of her name and address to that of a couple with an adverse credit history. Although the complainant lived in a different village and had a different post code, she shared the same surname, house number, street name and postal town as the third party involved.

The credit reference agency was able to establish a disassocation between the two parties on the basis of the complainant's first name and post code. This action had the result of removing the adverse account information from the complainant's credit file.

Case 25

In 1989, whilst living with her parents, the complainant had her handbag, which contained credit cards and identification, stolen. The theft was reported to the police. The stolen items were used to make a fraudulent application for credit in a shop and several hundred pounds worth of goods were purchased. Upon receiving a bill for these goods, the complainant contacted the finance company and the fraud was revealed. After writing a number of letters to the finance company the complainant received no further demands for payment and assumed that the situation had been resolved.

In 1993, the complainant's mother had a credit application refused. She checked her credit reference file and found that the fraudulent account opened in 1989 appeared as a default against her daughter's name, and thus on her own credit reference file. At this point, both mother and daughter complained to the Registrar.

It was revealed that, whilst the finance company's records showed the account as a

fraud, established procedures had not been followed with regard to notifying the credit reference agencies. The information was removed from the files immediately and assurances were given that such a situation should not arise again.

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 Crown Courts, or their equivalent in Scotland and Northern Ireland. They have usually been heard in the Magistrates' Courts.

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

(a) *Prosecutions*

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

Section 5(1):	Holding personal data without being registered or without having applied for registration. (Data users who fail to renew their register entries are also charged under this section.)
Section 5(2)(b):	Holding or using personal data for a purpose other than the purpose or purposes described in the register entry.
Section 5(2)(d):	Disclosing personal data to a person not described in the register entry.
Section 6(5):	Failure by a registered person to notify the Registrar of a change in the registered address.
Schedule 4 Para 12(a):	Intentionally obstructing a person in the execution of a warrant.

Prosecutions have been brought against 32 data users for criminal offences and a further 3 are awaiting hearing. The concluded cases are listed in Table 1.

As will be seen from Table 1, this year has seen further prosecutions under Sections 5(2)(b) and 5(2)(d) of the Act. These prosecutions are where data users have acted outside the terms of their register entries. These cases highlight the need for data users to review their register entries regularly. In that way, they can ensure that their current data processing activities are adequately covered by their registrations.

Offences under Section 5(1) are strict liability offences where it is only necessary to prove to the Court that the offence occurred. However, as far as Sections 5(2)(b) and 5(2)(d) are concerned, I am required to prove to the Court, beyond reasonable doubt, that the data user committed the offence 'knowingly or recklessly'. In the cases against Amnesty International British Section and Coats Viyella plc the Court concluded that the data users had not acted recklessly.

It is essential to clarify how "recklessly" should be interpreted in the context of the

Data Protection Act. For this reason, I have asked the Stipendiary Magistrate in the Amnesty action to state a case for the opinion of the High Court. This is the procedure which I used in the Griffin case, reported fully in my last Annual Report. Whatever the outcome, I am not seeking to change the verdict in the Amnesty case. I aim merely to clarify a point of law. It is likely to be some time before the case is dealt with and a more detailed analysis will be included in a subsequent Annual Report.

Table 1: Prosecutions in the Year to 31 May 1994

Section of the Act	Data User	Court	Date	Result/Fine £	Costs £
5(1)	Ragdale Hall (1990) Limited	Melton and Belvoir	08/06/93	100.00	50.00
5(2)(b)	Institute of Advanced Motorists Limited	Brentford	14/06/93	500.00	700.00
5(1)	The Bow Group	Marylebone	18/06/93	Conditional Discharge	577.50
5(2)(b)	Anthony Green & Company Limited	Marylebone	09/07/93	2,000.00	550.00
5(1)	Dr Roshan Kamrundin Hirani	Loughborough	13/07/93	60.00	40.00
5(1)	Andrew James Luxton t/a T.D. Hussey & Son	Honiton	14/07/93	175.00	325.00
5(1)	Neil Bannister	Bedford	20/07/93	200.00	550.00
5(1)	Glenn Paul Bugden	Southampton	23/07/93	75.00	25.00
5(2)(b)	Amnesty International British Section	Clerkenwell	29/07/93	Acquittal	Nil**
5(2)(d)	Amnesty International British Section	Clerkenwell	29/07/93	Acquittal	Nil**
5(1)	Stuart Simpson Gearty	Dundee Sheriff	18/08/93	50.00	0.00
5(1)	Trevor Wayne Lowe t/a Select Publications	Brighton	27/08/93	Conditional Discharge	500.00
5(1)	Kosmar Villa Holidays plc	Enfield	09/09/93	300.00	500.00
5(1)	Status Investments Limited	Sheffield	14/09/93	500.00	282.50
5(1)	Applied Data Base Limited	Morley	21/09/93	300.00	175.00
5(1)	Powerpen Limited	Marlborough Street	29/09/93	Conditional Discharge	100.00
5(1)	Medic International Limited	West London	22/11/93	300.00	200.00
5(1)	Marshall Control Systems Limited	Leeds	24/01/94	100.00	1,034.13)*
5(1)	Marshalls plc	Leeds	24/01/94	100.00	)
5(1)	Fielden Engineers Limited	Leeds	24/01/94	100.00	)
5(1)	Marshalls Hard Metals Limited	Leeds	24/01/94	100.00	)
5(1)	Halifax Tool Company Limited	Leeds	24/01/94	100.00	)
5(1)	Bondhappy Limited	Huyton	24/01/94	500.00	500.00
5(1)	Hoyers (UK) Limited	Huddersfield	14/02/94	Conditional Discharge	141.00
5(2)(b)	Viking Direct Limited	Leicester	11/03/94	1,000.00	1,221.34)*
5(2)(b)	Viking Direct Limited	Leicester	11/03/94	1,000.00	)
6(5)	Viking Direct Limited	Leicester	11/03/94	500.00	)

Section of the Act	Data User	Court	Date	Result/Fine £	Costs £
5(1)	Mohammed Hafeez t/a Star Video	Wick Sheriff	14/03/94	150	0.00
5(1)	Star Computer Services (UK) Limited	Rugby	15/03/94	500.00	461.12
5(1)	The Mosby Year Book Europe Limited	Clerkenwell	15/04/94	200.00	230.00
5(1)	Portland Publishing Limited	Harrow	19/04/94	1,000.00	300.00
5(1)	Berkeley Garage (Southampton) Limited	Marlborough	19/04/94	1,500.00	500.00
5(2)(b)	Coats Viyella plc	Wells Street	20/04/94	Acquittal	Nil
5(1)	Manchester Visionplus Limited	Manchester City	29.04.94	1,000.00	250.00
5(1)	Square Deal Motors	Falkirk Sheriff	04/05/94	Admonished	0.00
5(1)	Royal National Theatre	Horseferry	05/05/94	Conditional Discharge	376.00

* Joint costs
** Appeal lodged by the Registrar

(b) Supervisory Actions

An Enforcement Notice has been served against Linguaphone Institute Limited relating to obtaining information. This notice has been appealed to the Data Protection Tribunal.

A Preliminary Enforcement Notice has been served on Dixons Stores Group Limited. This relates to complaints which I have received from individuals who have informed the company that they do not wish to receive marketing literature, but who have been sent such literature despite their requests. A Preliminary Notice warns the data user that I intend to use my enforcement powers and the data user has a chance to respond to this. I am currently awaiting representations from Dixons Stores Group Limited in reply to the Notice.

(c) Appeals to the Data Protection Tribunal

Last year I reported that four appeals were awaiting hearing before the Data Protection Tribunal. The data users concerned were: Consumerlink Limited; Innovations (Mail Order) Limited; Trent Mail Order Company plc and International Correspondence Schools Limited. All four of these appeals related to the fair obtaining requirement of the First Data Protection Principle in the context of direct marketing. All four of the appeals have now been resolved.

The appeal by Consumerlink Limited was resolved by agreement and there was no formal hearing before the Tribunal. The case had arisen following concerns about the use of product registration cards to obtain information which was subsequently used for the purposes of direct marketing. On the early versions of these cards the use of data for this purpose was not made clear to respondents. Although the cards had been re-designed to ensure that the uses of the information were clearly explained, a number of early cards continued to be returned. This was because such cards were packed with consumer goods and would be returned as the goods were sold. In addition there remained the question of the information already obtained.

My staff had had lengthy discussions with Consumerlink Limited about the use of data from the early cards. The company had originally agreed to expunge the data obtained on the cards by the beginning of 1992. However it had subsequently been unwilling to comply with this agreement and argued that it should be able to retain the data indefinitely. I took the view that this was not acceptable and in 1992 served an Enforcement Notice on the data user restricting the use of the disputed data. Before the Tribunal hearing took place, agreement was reached for such a restriction. That agreement was placed before the Tribunal. Consumerlink Limited has recently confirmed that none of the information obtained from the early versions of the cards is now used for mailing purposes.

The case of Innovations (Mail Order) Limited was heard by the Tribunal in September 1993. The Tribunal ruling supported my view that those obtaining information from individuals should explain any uses of data which are not obvious before the information is obtained. A full report of the case is in Section 4.

The other two pending appeals which also related to the same subject matter were settled without hearing following the decision in the Innovations case.

As noted above, an appeal to the Tribunal has been lodged against an Enforcement Notice served on Linguaphone Institute Limited. This appeal is currently awaiting hearing. This appeal may be dealt with by way of written submissions as it deals with similar issues to those in the Innovations case.

(d) Refusal of Applications to Register

During this year seven applications for registration have been refused. In each case, the refusal was carried out under Section 7(2)(a) of the Act. This Section concerns the situation where the particulars proposed for registration would not give sufficient information as to the matters to which they relate.

Section 19 of the Act gives a right of appeal to the Data Protection Tribunal against a refusal by the Registrar of an application by that person for registration. Such appeals should be served on the Tribunal within 28 days of the date of service of the notice. There have been no appeals lodged with the Tribunal within the specified time limit in any of these cases.

(e) Monitoring Compliance with the Act

This work, which involves the Investigations Department, has been undertaken in three specific circumstances.

(i) *Failure to Renew Register Entries*

A new system has been established to follow up those data users who fail to renew their register entries. A fax message is sent to a selection of such users who seem likely to need to re-register. Over half of those targeted in this way have responded either by re-registering or explaining why re-registration was not required.

Those who do not respond to the fax, or who do not respond satisfactorily are visited by investigation staff. Where such a visit is made then it is normal practice, given evidence to show that the organisation is not registered and should be, for a prosecution to be mounted. Several such cases are currently being considered for prosecution. A recent prosecution which arose in this way led to a fine of £1,500. This does put the £75 fee for a three year registration into some perspective.

(ii) *"Gone Aways"*

Experience shows that a number of failures to renew arise because data users fail to notify changes of address. This is an offence under the Act.

Some trials have been carried out into locating new addresses and following-up these data users. Results so far show that over one-third of these data users are no longer trading. On the other hand a roughly equal number have renewed their register entries and the remainder are still awaiting final checking.

(iii) *Trawling for Unregistered Data users*

Again a new initiative has been tried. This involves investigations staff telephoning potential data users in selected areas. This activity has generated spin-off local media coverage which has helped to inform those who lack knowledge of the Act. On average, about 13% of those contacted so far should have registered, but had failed to do so.

(f) Use of a Warrant

The conduct of investigations has required the obtaining of two search warrants during the last year. The first search warrant was obtained and executed after a demand for access failed and other pre-requisite warrant conditions had been met. A prosecution for obstruction of the execution of this warrant is in hand. In the case of the second warrant, no prior demand for access was made, however it did not prove necessary to execute the warrant.

7 The Data Protection Register

Last year I commented on a "disturbing backlog" which had built up in registration work. This primarily occurred because 1992-93 was the peak registration year (in a three year cycle) and this had coincided with a real reduction in grant-in-aid. The backlog has now been significantly reduced, largely as a result of improved working practices. The reduction has been achieved despite a busier than anticipated year. In particular, the number of new applications for registration was higher than expected. Difficulties remain, however, in bringing registration amendment requests up to date and more staff are having to be put on to this work.

I am reviewing the legal and practical arrangements for the registration of partnerships. This may lead to some alteration in the way these registrations are dealt with. To date I have been prepared to accept registrations in the name of the partnership. Whilst this has considerable advantages administratively it has also given rise to problems where partnerships have been dissolved or partners have split up. If any alterations are proposed as a result of the review I will notify those affected in due course.

More than 23,000 new applications to register have been received together with a similar number of requests for amendment of register entries and almost 28,000 renewal requests. In addition over 6,000 applications were made to revive entries on the register which had lapsed. Over the year, the number of entries on the register has grown from 166,327 to 188,766.

I remain concerned about the number of entries which are not renewed at their expiry date. Also, a number of data users are failing to inform the Office of a change in business address. A more avid pursuit of those organisations failing to meet their registration obligations was recommended in the National Audit office Report referred to in Section 11. Some actions being taken are described in Section 6(e).

8 Informing People About the Act

(a) Strategy

The strategy remains to concentrate on pro-active public relations work; the provision of information, advice and educational materials; and more regular contact with and support for trade and other representative bodies, libraries, citizens advice bureaux, schools and colleges. When the budget allows for any advertising campaigns this ranks as a bonus.

As ever, there is a problem as to how to direct effort as between individuals and data users. The television advertising campaign last year was directed at individuals. It resulted in an initial massive increase in complaints and a longer term lifting of complaints numbers. The balance of effort this year has been more towards informing small data users. In line with this, a new approach is being made to computer suppliers seeking their co-operation in distributing information about the Act.

Towards the end of the year, an educational publisher was contracted to produce formal teaching materials for use in secondary schools and these are scheduled to be available for the new academic year in September 1994. The long term objective is to see a new generation knowledgeable about data protection emerging to adulthood in a few years time.

(b) Media Relations

Interest in data protection remains high in all sections of the media. The interest may be general and express itself in requests for information or for articles on the Act. Or it may be more specific, arising from some wider news story, for example, concerning identity cards or the security of personal financial data.

The Office pursues a very open policy and journalists are encouraged to talk with the staff most concerned with a particular issue. Relevant information and comment is given wherever possible.

The Office issued 20 news releases during the year and recorded 1,262 press mentions. Staff carried out 35 radio and 4 television interviews.

(c) Publications and Educational Materials

Demand for publications and educational material reached an all-time high. In the past year, the Office has distributed over 105,000 copies of the introductory leaflet "What is Data Protection?", 31,256 sets of the eight Guidelines booklets and 48,405 copies of the individuals' rights leaflet "If there's a mistake on computer about you". Also, 48,173 registration packs have been provided in addition to 6,049 special registration packs for schools. The information pack for students has also proved very popular with 30,593 copies being sent out.

The annual "Update" newsletter was sent to registered data users in December. As in the previous year, this contained a year planner/poster reminding data users of the Data Protection Principles. Some 178,000 copies of this newsletter were mailed to contacts on the register with a further 7,700 copies being distributed in response to specific requests.

Interest in the 15 minute introductory video on data protection continued. More than 8,500 copies were distributed including those sent in response to the advertising campaign referred to below.

A mailing to all public libraries ensured that they now have a range of up-to-date publications, including in many cases the data protection video. A bookmark produced specifically for distribution through libraries, reminding data subjects of their rights under the Act, was enthusiastically received and more than 120,000 were distributed throughout the year.

(d) The Enquiry Service

This service is setting new records each year both in the number of enquiries handled and in the productivity of the staff involved. Last year staff handled 52,010 telephone calls and 19,747 letters. In the last few months of the year, telephone calls to the Enquiry Service have been running at a rate of around 70,000 per annum.

(e) Conferences and Seminars

Policy staff are heavily involved in giving presentations at the request of conference organisations and data users. They also provide the speakers for the Office's own series of seminars which were begun on an experimental basis last year.

The demand for speakers from the Office continues to increase. Wherever possible these requests are met. As a result, 160 presentations were given to a wide variety of audiences throughout the United Kingdom. This compared with around 100 presentations in the previous year.

Three separate series of the Office's own introductory seminars on the Data Protection Act were held for data users in both the private and public sectors. The seminars were held at various locations around the country in June, November and March. They were enthusiastically received, with nearly all venues being heavily oversubscribed. There is a considerable waiting list of those wishing to attend future seminars.

(f) Advertising

An advertising campaign was carried out throughout the month of March. This was aimed at encouraging small businesses to find out whether or not they needed to register. The campaign was primarily founded on small advertisements in selected national and regional daily newspapers. Space was also taken in particular trade publications, such as Caterer and Hotelkeeper, Estates Gazette and Motor Trader, and in a selection of computer magazines aimed at personal computer owners or purchasers.

The advertisements incorporated a coupon to enable respondents to apply for a free copy of the data protection video and the information pack for small businesses. Over 6,000 responses were received, and analysis of the results is presently being undertaken to relate this response to geographical areas and/or particular business sectors. This information should then provide useful guidance on where best to direct promotional activities of this type in future.

(g) Exhibitions

Less effort was directed this year to exhibitions. Stands were taken at only 3 events. There was a good level of interest at each of these.

9 Research into Attitudes and Awareness

Once again research has been carried out amongst the general public and amongst both large and small data users. More detailed results from this year's survey are included in Appendix 5, together with comparative figures from the previous two years. These surveys, which test public attitudes as well as awareness of data protection issues, have been carried out on a regular basis since 1986.

(a) Public Attitudes and Awareness

"Protecting people's rights to personal privacy" remains in fourth position in the table of issues which people consider as very important and has the same proportion of support (66%) as last year. It follows "preventing crime on the streets" (86%), "improving standards of education" (79%) and "unemployment" (73%). It leads "protecting freedom of speech" (57%), "inflation" (53%), "equal rights for women" (53%) and "protecting the rights of minority groups" (36%).

Awareness amongst the public of the Data Protection Act and the Data Protection Registrar has increased significantly. Total awareness of the Act increased from 38% in 1993 to 47% in 1994. Semi-prompted awareness of the Registrar increased from 35% to 45%. In all, total awareness of the Act and/or the Registrar rose from 53% in 1993 to 64% in 1994.

Some confirmation of this last figure can be drawn from a "Direct Mail Trends Survey" prepared for the Direct Mail Information Service by BMB International Limited. This survey found 61% of respondents aware of the Data Protection Act in 1993. This compared with figures of 49% in 1991 and 27% in 1987.

(b) Data User Awareness

The data user research distinguishes small users (organisations with fewer than 50 employees) from large users (those with 50 employees or more).

The proportion of small organisations using a computer or computer bureau has remained virtually the same in 1994 (54%) as in 1993 (53%). Similarly the proportion of small organisations holding personal records on computer has also remained steady (50% in 1994, 51% in 1993).

Awareness of the Data Protection Act remains high (86% of small organisations and 97% of large) and at similar levels to last year. However, there has been a fall in semi-prompted awareness of the Data Protection Registrar amongst both small (54% to 46%) and large (75% to 61%) organisations between 1993 and 1994.

In general, the figures seem to indicate some general falling off in awareness of the more detailed obligations of the Act and the rights it confers on individuals. Plainly there is still a considerable task ahead in informing and educating data users.

10 International Activities Outside The European Union

(a) The XVth International Conference of Data Protection and Privacy Commissioners

It was my pleasure this year to host the Annual Conference of Data Protection and Privacy Commissioners. This event – the fifteenth- was held in Manchester from the 28th to 30th September 1993.

Her Royal Highness, The Princess Royal, kindly honoured us by opening the Conference. Her Royal Highness's opening address, which embraced both the international dimension of the event and the complex nature of many data protection and privacy issues, gave the Conference a thoughtful and stimulating start. I am grateful also to Mr Peter Lloyd, Minister of State at the Home Office who spoke at the farewell dinner. Mr Lloyd expressed the Government's support for data protection legislation and outlined its policies in respect of developments in the European Union.

I should also like to thank the Cities of Manchester and Chester and in particular the Lord Mayors of those cities for their hospitality and support.

The developments in this Conference mirror the advance of concerns about data protection and privacy issues across the world. The first conference I attended, in 1984, comprised a small group of people from a handful of countries. We met around a single table in a room over the stables of the Spanish Riding School of Vienna. In 1994, over one hundred delegates from twenty-six countries filled the Council Chamber of Manchester Town Hall. I was pleased to welcome so many delegates, including not only data protection and privacy commissioners and their staff, but observers from international organisations and others with a professional interest in data protection and privacy.

The Conference provides Commissioners with a valuable opportunity for the exchange of experiences and ideas and helps to promote understanding and closer co-operation on an international scale. As computing systems are developed which stretch beyond national boundaries, such understanding and co-operation become increasingly important. For observers too the Conference provides a useful opportunity to meet the regulators and discuss data protection and privacy issues with them.

The theme of the Conference was "All about people". Among the issues considered were: freedom of the press and privacy protection; identification of individuals through the use of personal identification numbers; the privacy implications of genetic testing; the use of publicly available information; and surveillance by technological means.

The Conference was designed to stimulate thought by presenting opposing views on the various subjects. Thus, speakers with data protection and privacy backgrounds and commitments were challenged by those whose views and interests pulled in other directions. Speakers were drawn from a number of different countries and came from both the public and private sectors.

The diverse backgrounds and interests of speakers were reflected in their presentations. These offered fresh insights into current issues and challenged delegates to reappraise accepted data protection and privacy approaches. These formal presentations stimulated lively debate both inside and outside the conference chamber. I thank all of the speakers for the thought-provoking contributions they made to the Conference. From the many favourable comments made by delegates, the conference clearly provided a valuable and educative exchange of views. It is my intention to publish the proceedings of the Conference.

Many people, both inside and outside my Office contributed to the Conference through organisational work or providing facilities and hospitality. I am grateful to them and delighted to have been associated with this significant event in my final year in office. I wish our Dutch colleagues a very successful event later this year in The Hague.

(b) The Council of Europe

The Deputy Registrar attends the Council of Europe Project Group on Data Protection. This group is instrumental in preparing recommendations for the Committee of Ministers to approve. The recommendations are designed to assist the implementation of the Council of Europe Convention on Data Protection.

Early in the year considerable effort was expended in preparing comments for the Home Office on the draft Recommendations on Statistics and Medical Data and also on a proposal to review the Police Sector Recommendation. The text of the Recommendation on Medical Data has yet to be finalised. The Working Party on Insurance met for the first time this year and began consideration of a draft Recommendation on which comments have been submitted to the Home Office. Approval of the Telecommunications Recommendation by the Committee of Ministers is awaited.

(c) Other International Contacts

Two of my staff attended the OECD Ad Hoc Meeting on the Protection of Personal Data and Privacy held in Paris.

Two meetings of the British Data Protection Authorities (Guernsey, Jersey, the Isle of Man and the United Kingdom) took place, one in London and one in the Isle of Man.

One of my Assistant Registrars presented a paper at the International Medical Informatics Association Working Conference in Amsterdam and another Assistant Registrar presented a paper at the Conference of the Universal Federation of Travel Agents Association held in San Juan, Puerto Rico.

This year my office has received visitors from Albania, Belgium, Finland, Ireland, Israel, the Netherlands, South Africa and Spain. A Commissioner and members of staff from the Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection authority, joined members of my staff on visits to research laboratories in Cambridge. Subsequently, the Deputy Registrar and Senior Assistant Registrar spent two days at the offices of the CNIL in Paris. Two members of staff also visited the headquarters of Interpol in Lyon, France.

I should like once again to record my gratitude to the Data Protection Authorities of other countries for their continuing co-operation and assistance during the course of the past year.

11 Organisation and Finance

(a) The House of Commons Committee of Public Accounts

I gave evidence to the Committee of Public Accounts on 24 November 1993. The Committee was considering a report on my Office prepared by the Comptroller and Auditor General*

This National Audit Office (NAO) Report considered the activities of my Office and reached a number of conclusions. These conclusions are in Appendix 6. The Report did not criticise the efficiency of my Office, but rather recommended that additional work should be undertaken. The NAO recognised that action on its recommendations was subject to constraints both in the resources available to the Office and in the powers of the Registrar.

The discussion with the Committee of Public Accounts ranged across the policies I have set for the Office, my powers and the resources available. I have provided the Committee with a costing of some possible responses to the NAO recommendations and a breakdown of how grant-in-aid is currently allotted to meeting my various statutory duties.

The Committee has published the minutes of evidence of the meeting of 24 November** but has not at the time of writing (mid-June 1994) published its conclusions on either the NAO report or the meeting.

(b) Grant-in-Aid

I have had occasion over the last two years to draw attention to real reductions in the grant-in-aid which were causing considerable difficulties. The difficulties were compounded by the general development in data protection activity, by a peak registration year and by a surge in the number of complaints received. The result has been a rundown in some activities and enforced transfer of staff from others.

I am pleased to report that the Home Office has responded to my concerns. The grant-in-aid allocated for 1994-95 is 9.8% higher in real terms than that for 1993-94. In the current public spending climate, this is very welcome. The increased grant-in-aid should give a much firmer financial basis for the new Registrar for the coming year's work. However, the new grant-in-aid is still less than that requested. It will underpin current priorities and work programmes, but is unlikely to allow any significant changes or enhancements to these, for example to meet the NAO recommendations referred to above.

(c) "Open Government" and Office Resources

In July 1993 the Government published its White Paper on Open Government (see

* The National Audit Office, Report by the Comptroller and Auditor General, "Data Protection Controls and Safeguards". London: HMSO. 20 August 1993.
** House of Commons Session 1993-94, Committee of Public Accounts, "Data Protection Controls and Safeguards". Minutes of Evidence 24 November 1993. London: HMSO. ISBN 0-10-273094-6.

Section 3(f). This makes a move towards greater openness in respect of public sector information. It envisages that the Registrar's Office will take on responsibility for administering a new subject access right to information in manual records.

There will be resource implications in taking on this extended role. I understand that the resources being made available to the Parliamentary Commissioner for Administration will permit him to employ up to 50 staff, if necessary, in ensuring compliance with the Open Government Code of Practice. He has assumed that a majority of the new complaints he receives will raise subject access issues. At present, all figures must of necessity be tentative. It remains to be seen what experience will be in administering the new subject access right, but clearly there will need to be some addition to the Registrar's resources.

(d) Results for the Year

Expenditure for the year was £3,448,778. Receipts from registration fees amounted to £4,415,407. In addition, a further £78,450 was received from a variety of sources including interest earned on funds temporarily invested during the year.

The Statement of Account for the year ended 31 March 1994 as certified by the Comptroller and Auditor General is in Appendix 7. I am grateful to the National Audit Office for processing the audit rapidly so that the final account could be included with this Report.

(e) Recovery of Expenditure

The Data Protection Act 1984 lays down in Section 40(7) that registration fees are set by the Secretary of State who "shall have regard to the desirability of securing that those fees are sufficient to offset the expenses incurred by the Registrar and the Tribunal in discharging their functions under this Act and any expenses of the Secretary of State in respect of the Tribunal". Fees payable shall be prescribed by regulations made after "consultation with the Registrar and with the approval of the Treasury". The Secretary of State has the power to recover past deficits.

Under the Act, the Registrar has a duty to pay all receipts into the Consolidated Fund. Under a direction contained in a Treasury Minute of 27 October 1986 under powers conferred under Section 2(3) of the Public Accounts and Charges Act 1981, I am required to make those payments to the Home Office as appropriations- in-aid. No income from registration fees is available to my Office. The funding of the Office is by grant-in-aid as referred to above.

To assist the Secretary of State in securing that fees are sufficient to offset expenses, I planned to recover all the relevant expenses (including set-up costs) in cash terms by 31 March 1996. That is, by that date, actual receipts would recover actual expenditure. I published this plan in my Sixth Annual Report to Parliament (June 1990) as part of a corporate planning statement setting out corporate objectives and strategies. The plan foresaw the need for increases in the registration fee beyond the £75 level now pertaining. In the event, in the terms of this plan, those increases have not, so far, been necessary.

The following table gives the actual receipts and expenditures of my Office since its inception. It shows that, in cash terms, the objective I set has been achieved two years ahead of schedule and without any further increase in the registration fee. Schools registrations have been significant in this achievement. Forecasts for future years based on projected income and grant-in-aid suggest that the Office will now make substantial over-recoveries in cash terms.

Since publishing the financial plan, I have been asked by the Home Office to provide information as to the effect on fees if the Office were required to operate an accruals based accounting system. Discussions on this matter are currently in progress.

Financial Position to 31 March 1994

Year Ending 31 March	Office Expenditure £'000	Other Expenditure £'000	Receipts £'000	Cumulative Financial Position £'000
1985	308	31	0	(339)
1986	1,696	58	424	(1,669)
1987	2,422	72	2,757	(1,406)
1988	2,650	60	930	(3,186)
1989	2,624	60	1,294	(4,576)
1990	2,975	67	5,428	(2,190)
1991	3,153	83	2,068	(3,358)
1992	3,402	95	2,425	(4,430)
1993	3,723	78	7,842	(389)
1994	3,449	83	4,494	573
Totals to 31/3/94	26,402	687	27,662	573

Notes

1. "Other expenditure" includes that incurred in respect of the Data Protection Tribunal, the Data Protection Registrar personally and related Home Office costs.
2. "Receipts" include registration fees and other receipts such as interest on unallocated grant-in-aid in hand invested at overnight rates.

12 Conclusions

In these conclusions, I largely repeat the views I gave at the opening of the XVth International Conference of Data Protection and Privacy Commissioners. For I believe them still to be relevant. Now, as then, I am tempted to look backwards as well as forwards. For the rapid developments in technology, techniques and the uses of personal data evident in this Report had their origins some time ago.

I am minded to start in 1961. It is convenient because computing was at one of its many watersheds and because it was when I first entered the computing industry. Things computing were beginning to take off. I did my programming training on DEUCE, a machine whose data storage comprised pulses of sound passing through columns of mercury. It was programmed in binary and you could do black magic with it – but very slowly. Fortunately, for anyone wishing to do serious commercial computing, magnetic core storage machines had recently arrived and were progressively taking over from punched card systems.

We were all new into computing but we were weavers of dreams. Our dreams were of a world of automatic processing of information where machine would communicate with machine, system with system, computer user with computer user. Not only were we new in the game, we were also naive, for of course we were far from having the capacity to make our dreams reality.

But that capacity has increasingly become available. Perhaps a good illustration of this is the storage of information. In the early sixties we were looking at a cost of £0,5 for a character of storage with stores of 64,000 characters being considered large. In a small office like ours, we recently bought a storage device with a capacity of 4,000,000,000 characters at a price of £0,000003 per character.

By the mid sixties, our dreams, flimsy as they were, were becoming others' nightmares. They looked ahead with trepidation to this automated world where they foresaw that much of the information being automatically processed and exchanged would be about individuals. They saw a threat to the privacy of individuals.

It was not only civil rights protagonists who saw this threat. It was quickly recognised by computing professionals. On a number of occasions before becoming Registrar, I led computing industry discussions of this problem. Those discussions were not negative. There were many computing professionals, perhaps a majority, who expressed their concern and their support for data protection legislation through professional and other bodies such as the British Computer Society, the Institute of Data Processing Management and the National Computing Centre.

As a result of all these concerns, during the seventies and eighties we have seen data protection come onto the political and legislative agenda in an increasing number of countries. Those responsible for implementing the resultant data protection legislation have made some progress. Many problems have been solved for many individuals. Legislators have been convinced by argument that they should introduce data protection facets into other legislation. Computer users in the public and private sectors, have been educated, persuaded and, where appropriate, coerced, into setting up good practices in their use of information about individuals.

But we have far to go. New technologies and new uses of personal data flow steadily out of the creative and imaginative minds of mankind. Only a few years ago we would not have forecast that we might be discussing many of the issues outlined in this Report.

So, whither the dream and whither the nightmare? The dream is racing towards reality. A glance at this Report and at the present world of computing – with its sophisticated data collection devices, its massive data banks and its burgeoning communications facilities – shows the dream taking shape all around us. The nightmare increasingly disturbs our sleep.

We are heavily into the problem of balancing conflicting public policies. How does privacy balance against freedom of speech, or the health of the nation, or the prevention of crime, or economic benefit?

In setting appropriate balances it is possible to see the need for care in the handling of information about people in different ways. At one end of the spectrum there is the natural human instinct for some space of one's own. At the other there is the issue of the power which knowledge and control of information about people might place in the hands of a totalitarian state. This latter consideration seems alien to a country with the history of the United Kingdom. But we do not need to travel far from these shores or go back far in time to see that totalitarian states can occur. Indeed, the history of the world is littered with totalitarian states. Justice, freedom and democracy are fragile flowers.

We therefore need to evaluate the benefits which can come from the use and exchange of personal data and weigh these carefully against the risk of loss of privacy. Will the regimentation and monitoring of facts – and sometimes fancies – lead to the regimentation and monitoring of people? Will individuals lose the ability to say this is my space; this is my information; and this is none of your business?

The answers to these questions will be determined by the decisions of politicians and parliaments. They will not be easy decisions. Those who have responsibilities for data protection and privacy matters must make their own thoughtful, measured, but powerful contribution to the discussions and decisions which will take place. I hope that my Office has been able to make a useful contribution to this necessary debate.

E.J. HOWE
DATA PROTECTION REGISTRAR
JUNE 1994

Appendix 1

Personal Data held within The Finance Industry: Some Implications of The First Data Protection Principle with regard to confidentiality

> *"The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully."*
> (1st Data Protection Principle) (1)
>
> *"... in determining whether information was obtained fairly regard shall be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed."*
> (Statutory interpretation of the 1st Data Protection Principle) (1)

INTRODUCTION

1. This paper relates to the fair and lawful obtaining and processing of personal data within the finance industry. It primarily addresses the confidentiality of individuals' details and account data and the disclosure and use of such data for credit referencing and marketing.

2. In the Ninth Report of the Data Protection Registrar to Parliament in June 1993, the Registrar published his views on the requirements of the First and Second Data Protection Principles to obtain, hold and process personal data *lawfully*. The Registrar considers *unlawful* to mean:

> *"... something which is contrary to some law or enactment or is done without lawful justification or excuse."*

3. This is a broad definition and includes not only breaches of the criminal law, but also breaches of civil law. Thus it may be that if personal data are used for example, in breach of copyright, in breach of contract or in breach of a duty of confidentiality that the processing of such information will be *unlawful*.

4. In circumstances where an obligation of confidence arises between a data user and a data subject in the finance industry, it is the Registrar's view that it is *unlawful* for a data user to use data for a purpose other than that for which the information was provided except in certain circumstances permitted by law, such as with the consent of the data subject. Where such a use involves the processing of personal data, then this may entail *unlawful* processing within the meaning of the First Data Protection Principle.

(1) Data Protection Act 1984 Schedule 1

AN OBLIGATION OF CONFIDENCE

5. The Registrar's view is that financial institutions are subject to an obligation to maintain details of relationships and financial transactions between themselves and those individuals with whom they deal as confidential. Confidentiality policies and procedural instructions should be made available to, and practised by, members of staff. The following test may be applied in considering whether a duty of confidence exists:

   (a) The information provided by the confider must in fact be confidential.

   (b) The information has been obtained in circumstances which impose an obligation on the confidant to respect the confidentiality of the information (for example: An application form may indicate that the information supplied will be kept confidential by the recipient, or, an individual supplying information may do so on the understanding, or with the legitimate expectation, that it will be kept confidential).

6. The Registrar considers that this duty of confidence applies, amongst others, to banks, building societies, the issuers of credit or charge cards, finance houses (and leasing companies) and insurance companies. This list is not exhaustive, the test in paragraph 5 above may apply to a wide range of organisations.

QUALIFICATIONS TO THE DUTY OF CONFIDENCE

7. Some aspects of the general law of confidence as applied to a bank were considered in the case of *Tournier v National Provincial and Union Bank of England* in 1924. Although a landmark case, the judgments did not *define* the common law duty of confidentiality but reflected the general law and set out four exceptions under which the bank could legitimately disclose information about its customer:

   (a) Where disclosure is under compulsion by law.

   (b) Where there is a duty to the public to disclose.

   (c) Where the interests of the bank require disclosure.

   (d) Where disclosure is made by the express or implied consent of the customer.

8. The *Tournier* exceptions are largely a matter of the usual law of confidentiality. The only exception which is perhaps not fully reflected in the general law of confidence is when disclosure is in the interests of the bank. It is the view of the Registrar that the usual law of confidence applies to organisations in the finance industry but that they may be able to rely on the *Tournier* exceptions to justify certain disclosures of information about individuals on their databases.

CONSENT

9. The most usual basis for the disclosure of personal data by financial institutions to third parties (including companies in the same commercial grouping) is that the individual has *consented* to such disclosures; the fourth of the *Tournier* exceptions. If an individual has consented to the disclosure of personal data relating to him or her then such disclosures are *lawful*. Proper records of consent must be maintained. However, where such consent has not been given, it is possible that the disclosures are *unlawful* unless other lawful reason for disclosure can be demonstrated.

10. An individual's consent must be given voluntarily, and s/he must not be coerced into giving it. In addition s/he must be fully aware of what s/he is consenting to for it to constitute proper consent. In general, if a financial institution gives an

individual notice of what it intends to do with personal data about that person, and s/he does not respond, the financial institution would **not** be entitled to assume that s/he had impliedly consented to the use of the information. In other words it is impossible to infer assent from silence alone.

CONSENT AS A CONDITION OF BUSINESS

11. It has been argued that it is possible for a financial institution to require the consent of an individual to the disclosure of personal data to third parties, either to other organisations for marketing purposes or for the disclosure of financial information about particular accounts to credit reference agencies, as a condition of the contractual arrangement between the financial institution and the individual. Under current legislation, in particular the Unfair Contract Terms Act 1977, it would not be unlawful to impose such a condition. Any disclosures made in reliance on such a consent would not, therefore, entail the *unlawful* processing of personal data.

12. However, this position may change as a result of the EC Directive on Unfair Terms in Consumer Contracts. Article 3.1 of the Directive states:

> *"A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer"*.

13. A consultation document, *Implementation of the EC Directive on Unfair Terms in Contracts*, published in October 1993 by the Department of Trade and Industry proposes that the UK Government complies with the Directive through the introduction of regulations which will lie alongside the existing Unfair Contract Terms Act 1977. It is stated in the introduction to the consultation document that: *"The main effect of the Directive will be to introduce for the first time a general concept of fairness in the UK law of contract"*. The Registrar welcomes this development and believes that the view of fairness embodied in the Directive and consultation document is supportive of and consistent with the obligation of fairness as it applies to the First Data Protection Principle.

14. The proposed regulations follow the Directive quite closely. For instance, it is proposed that Article 3.1 be implemented as follows:

> *" 'Unfair term' means any term which contrary to the requirement of good faith causes a significant imbalance in the parties' rights and obligations under the contract to the detriment of the consumer, taking into account the nature of the goods and services for which the contract was concluded and by referring, at the time of the conclusion of the contract, to all circumstances attending the conclusion of the contract and to all other terms of the contract or of another contract on which it is dependent."*

15. Schedule 2 of the proposed new regulations sets out the matters to be considered in determining whether a term satisfies the requirement of *"good faith"*, as follows:

> *"In making an assessment of good faith, particular regard shall be had to*
>
> — *the strength of the bargaining positions of the parties,*
>
> — *whether the consumer had an inducement to agree to the term,*
>
> — *whether the goods or services were sold or supplied to the special order of the consumer, and*
>
> — *the extent to which the seller or supplier has dealt fairly and equitably with the other party whose legitimate interests he has to take into account."*

16. It is planned that the new regulations are finalised by the middle of 1994 and will become effective by 31 December 1994. Although the Registrar accepts that this Directive does not yet form part of the UK law, the scope for amendment to the proposed regulations is evidently somewhat restricted, not least by the central purpose of the Directive which is to: *"approximate the laws, regulations and administrative provisions"* of the different EC member states.

17. Under the proposed regulations an individual will be able to apply to a court to have a term of a contract declared unlawful and struck out of the contract because it fails to satisfy the test of good faith. Such a term is described as *voidable*.

18. It seems to the Registrar that to require individuals to agree to the use and disclosure of confidential information could cause a *"significant imbalance"* in the rights and obligations of parties to the *"detriment of the consumer"*, and such a term is potentially voidable by the courts. In the event that a data user processed personal data in reliance on a term which had been declared void the processing would be unlawful. However, even before a term were declared unlawful by the courts, if it failed to satisfy the test of good faith the Registrar could consider processing in reliance on it as *unfair* processing (see paragraphs 28 – 29 below).

THE USE OF PERSONAL DATA FOR MARKETING

19. The December 1991 edition of the *Good Banking* Code of Practice forbids the *disclosure* of personal data by banks, building societies and credit card issuers to other companies, including companies in the same commercial grouping, for the purpose of marketing in the absence of express consent. The Registrar considers that the protection given by paragraph 6.1 and paragraph 8.1 of the *Good Banking* Code of Practice (which forbid the disclosure of customer details generally other than within the *Tournier* exceptions; and which require express customer consent for disclosures of information for marketing purposes) has been undermined by the fact that many institutions employ *"host mailing"* techniques. By this technique, they mail selections of individuals on their own databases with offers of goods and services from other companies in their groups. The customer information is not disclosed to the other companies, although they may ultimately come into possession of it. A simple example of this might be where an institution mails a financial service offer on behalf of another company in the group. It does so only to those customers with a deposit account balance of at least £5,000. The other company will know that anyone responding to it is a customer of the institution concerned who has a deposit account with such a balance. This information will effectively have been passed to the other company without the customer's knowledge, let alone consent.

20. Whether or not a disclosure is involved, the duty of confidence also restricts the *use* of data. It is the view of the Registrar that customer information cannot lawfully be either *disclosed*, or *used*, for marketing purposes by third parties, including companies in the same commercial grouping, without the consent (see paragraph 10) of the customer. He considers that this is equally true for finance houses, store and charge card issuers and insurance companies as it is for banks, building societies and credit card issuers.

DISCLOSURE OF INFORMATION TO CREDIT REFERENCE AGENCIES

BLACK DATA

21. In 1988 a *Minute of Understanding* was agreed between the Data Protection Registrar and the Committee of London and Scottish Bankers, the forerunners of the British Bankers' Association. The *Minute of Understanding* was intended to apply during the period while the Jack Committee Report was being awaited. This agreement led to the disclosure of certain *black* information by banks to credit reference agencies.

22. The system set up by the banks in the light of the *Minute of Understanding* was that information about bank loans would be made available to credit reference agencies where an individual had fallen three months in arrears and had at that time received a communication from the bank warning that if no measures were taken to deal with the situation within a further 28 days, details of the delinquent account would be passed to credit reference agencies. In effect, anyone who fell four consecutive months in arrears on a loan with a bank would have this information passed to a credit reference agency.

23. The *Minute of Understanding* is no longer relevant. However, the system set up by the banks continues. It could be argued that making disclosures in such circumstances, subject to appropriate checks and safeguards, could fall within the third *Tournier* exception, as being within the interests of the bank. The argument would be that in circumstances where the bank has given the customer adequate opportunity to resolve the situation or reach some satisfactory agreement and has provided the customer with clear warning of the consequences of a failure to deal with a situation, then if the customer fails to respond, the bank is entitled to treat its own interest as overriding that of the particular customer, and make the disclosure.

24. There is, however, a strong argument to the contrary. The third *Tournier* exception has been narrowly construed by the Courts in the past. Moreover these are circumstances where it would have been possible to seek the consent of the individual to the disclosure. It is uncertain whether the Courts would consider that such a disclosure would fall within the exception. The interest of financial institutions would have to be weighed against the confidentiality of the relationship. If disclosures of individuals' details and account data to credit reference agencies cannot be made under the third *Tournier* exception the consent of the individual will have to be obtained in order to fall within the fourth exception. As explained in paragraph 11 above, disclosures and uses of data can always be made lawful by obtaining individual consent as a condition of contract.

WHITE DATA

25. The disclosure of *white* data to credit reference agencies is widespread. The Registrar does not consider that *white* data can be disclosed in reliance on the third *Tournier* exception and the consent of the individual will need to be obtained in order to comply with the fourth exception. Consent obtained as a condition of trade would not be unlawful under current legislation.

26. The effect of the EC Directive on Unfair Terms in Consumer Contracts on a term of a contract which required consent to the disclosure of data to credit reference agencies would have to be considered as described in paragraphs 17 and 18 above. It appears to the Registrar that the disclosure of *white* data could raise different questions of balance to the disclosure of *black* data. A contract term requiring consent to the disclosure of *black* data might not be in breach of the requirement of good faith. A contract term requiring consent to the disclosure of *white* data would in the Registrar's view, be voidable by the courts.

27. It is the Registrar's view that the individual should be able to decide whether or not *white* data about his or her accounts are made available to credit reference agencies. Credit grantors are at liberty to point out to individuals the advantages of allowing *white* data to be disclosed to credit reference agencies in that the individual will find it easier to obtain credit in future if a good borrowing history is established. Nevertheless, some individuals may prefer not to have their details passed to credit reference agencies and will accept that obtaining future credit may be more laborious.

FAIRNESS

28. The Data Protection Act requires that personal data shall be processed *fairly* as

well as *lawfully*. This paper has so far dealt with issues of lawfulness and the question of fairness has only been raised in the context of forthcoming legislation. However, the current practices raise questions as to the fairness of the processing of financial data.

29. Without reference to the proposed new regulations, the Registrar has also considered the implications of consent as a condition of business in the light of the obligation under the First Data Protection Principle to process personal data *fairly*. In this context he is mindful of the imbalance in power that exists between financial institutions and individual consumers and the fact that in a modern society individuals are effectively constrained to make use of the products and services which those institutions provide. The Registrar is concerned that a customer may have no choice but to give such consent as more and more institutions seek to impose the same conditions of trade. It may be unfair to *process* information to be used for third party marketing purposes or in order that that information may be exchanged with other institutions, via a credit reference agency, without the freely given consent of customers. In considering whether a breach of the fair processing requirement of the First Principle arises in particular cases, the Registrar will consider, *inter alia*, the degree of choice generally available to the individual and the nature of the product or service which he or she seeks.

IMPROVED STANDARDS FOR THE CONFIDENTIALITY OF PERSONAL DATA

30. In order to ensure that banks, building societies, credit and charge card issuers, finance houses, insurance companies and others in the finance sector do not breach the *fair* and *lawful* requirements of the First Data Protection Principle, the Registrar recommends that the following standards be adopted:

(a) Individuals be told each time information to be contained in personal data is requested from them all the non-obvious uses to which data about them and their accounts may be put. This includes what data may be disclosed to whom, and in what circumstances.

(b) Personal data should not be made available to third parties, either by direct disclosures or by the use of *"host mailing"* techniques, without consent. This consent should be in the terms of paragraph 10 above.

(c) It may be made a condition of an agreement that *black* data be made available to credit reference agencies in the terms set out in paragraph 22 above. Individuals would not generally have the opportunity to object to this or for the use of their personal data for the prevention or detection of fraud.

(d) Individuals may be invited to consent to their account details being passed to credit reference agencies when such information does not constitute *black* data as detailed in paragraph 22 above. The disclosure of *white* data and default data that does not yet meet the *black* data situation should only be disclosed to credit reference agencies with consent. This consent should not be made a condition of an agreement but should be the free choice of the individual, although financial organisations are at liberty to point out the advantages of allowing *white* data to be disclosed to credit reference agencies and the disadvantages of not so doing.

(e) The disclosure of data to credit reference agencies, and the retention of data by such agencies, in the course of a credit reference check when an application for a service is made, must be notified to the individual at the time of the application. No details of the type of service applied for, the amount of a loan or the repayment period should be recorded by credit reference agencies, although the fact of the search and the organisation that undertook it may be recorded.

31. This paper deals primarily with duty of confidence – there are other matters on lawfulness which are not covered by it. It is not an authoritative statement of the law as only the Data Protection Tribunal and the Higher Courts can provide this. The paper is designed to advise and inform. It cannot apply to all situations, nor will the examples given be valid in every circumstance. Where organisations need additional advice to help them comply with the provisions of the Data Protection Act 1984, the Registrar's staff will always endeavour to assist:

Office of the Data Protection Registrar (P&C4)
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Administration: (0625) 535711
Enquiries: (0625) 535777
Fax: (0625) 524510

27 JANUARY 1994

Appendix 2

Disclosure of Criminal Records for Employment Vetting Purposes – Consultation by The Home Office

Comments of the Data Protection Registrar

I welcome the opportunity to comment on the Home Office consultation paper on disclosure of criminal records for employment vetting purposes. I have commented previously on the National Criminal Records System in evidence to the House of Commons Select Committee on Home Affairs in 1990 and to the Efficiency Scrutiny of the National Collection of Criminal Records in 1991.

The disclosure of criminal records for vetting purposes raises some difficult questions of public policy, in particular how to achieve the right balance between the rehabilitation of offenders and the protection of vulnerable persons and property. In explaining the existing arrangements and how they have developed, the paper reveals inconsistencies and problems both of policy and practice.

Although the consultation deals only with employment vetting, disclosure for vetting in other areas (for example immigration) should not be ignored. Similar considerations apply.

It is undoubtedly true that, over the last few years, pressure has increased to make available details of an individual's criminal record in a wide variety of circumstances. From my position as Data Protection Registrar I see particularly the escalating use of "enforced subject access" whereby individuals are obliged to use their right of access under the Data Protection Act 1984 to obtain a copy of their criminal record from the police and pass it on to the prospective employer. I have argued frequently that this is an abuse of individuals' rights and should be prevented by criminal sanctions.

The growth of the use of enforced subject access highlights the need to review the current arrangements for disclosure. It is important to note that it is not only the criminal record which is a target for enforced subject access. National Insurance records too are being used increasingly as a source of information which can reveal a period spent in prison. Potentially, court registers could become a target as they become computerised.

If wider access is to be permitted, it is important that a proper framework is established within which such access can take place and that access outside that framework is effectively restricted. The consultation provides an opportunity to establish sound and long lasting arrangements for the future.

My detailed responses to the questions posed in the paper follow:

Question 1: Is it accepted that access to official collections of criminal records, including records solely of convictions, should in principle be restricted?

Response: There is strong argument that, on data protection grounds alone, access to

criminal records should be restricted. Article 6 of the Council of Europe Convention on Data Protection deals with 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.**"

The Explanatory Memorandum, in relation to Article 6, says that "while the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests. Categories of data which in all member states are considered to be especially sensitive are listed in this article."

The Data Protection Act 1984 refers to such sensitive data in Section 2(3). "The Secretary of State may by Order modify or supplement (the data protection) principles for the purpose of providing additional safeguards in relation to personal data consisting of information as to

(a) the racial origin of the data subject;
(b) his political opinions or religious or other beliefs;
(c) his physical or mental health or his sexual life; or
(d) **his criminal convictions**."

Whilst no Order has been made by the Secretary of State, the Data Protection Act 1984 recognises in Article 2(3) that there is something special about criminal convictions. It is not unreasonable to suggest that the safeguards envisaged in both the Act and the Convention should include restrictions on disclosure. My view is reinforced by Article 8 of the Draft EC Data Protection Directive which also includes similar restrictions.

Question 2: Should any non-conviction information continue to be disclosed for the protection of children? Should it be disclosed in any other contexts?

Question 3: Should non-conviction information include certain categories of acquittals or cases not proceeded with, as well as other factual 'intelligence'?

Question 4: Should minor convictions and cautions continue to be disclosed?

Response: These questions are related in that they all deal with what information should be disclosed in what circumstances. I can accept that there is an argument for disclosure of non-conviction information, which might include acquittals, in certain cases, and the protection of children clearly ranks highly. A thorough analysis needs to be done of all the circumstances in which information could be disclosed and a mechanism established by legislation by which decisions could be made in a consistent manner on precisely what information would be disclosed in each of those circumstances.

Question 5: What should be the broad criteria for authorising criminal record checks and what level of check would be appropriate in each circumstance?

Response: Paragraph 60(2) of the consultation paper refers to disclosure "to subjects within the terms of data protection principles". This leaves open the issue of forcing data subjects to use their right of subject access which I referred to in my introductory paragraphs. It cannot have been envisaged that such a procedure should be sanctioned, yet the way paragraph 60(2) is expressed might give the false impression that "data protection principles" would prevent it.

Apart from that, the general principles set out in paragraph 60 do seem to provide a good basis for disclosure policy. Equally, I would not question the three existing criteria

by which it is established when the public interest outweighs the general principles of confidentiality.

Deciding what are proper extensions to those criteria is, however, more difficult. For example, the "fit and proper person" requirement appears to be used in a number of different contexts. Without doing a detailed analysis of all those cases, it would be difficult to agree that disclosure of the criminal record would be justified in every case.

This underlines the argument for a detailed examination of all the circumstances under which criminal record information might be disclosed, which was touched on in my response to questions 2, 3 and 4. I would agree with the conclusion in paragraph 62, that the detailed interpretation would need to be done outside legislation but would suggest that is a strong argument for the independence of the body which is to do the interpretation.

Question 6: Should users be charged the full cost of vetting checks, and if so how should checks in the voluntary sector be financed?

Response: I have nothing against charging in principle provided that the charge is not borne by the individual. It is more a question of whether adherence to the principle of self-financing would be damaging to other public policy, for example, would a charge be a deterrent to proper checks being made? On that basis, the charge would need to be set at a reasonable level. This is also important from the point of view of deterring enforced subject access. If the charge for vetting were to be significantly higher than the £10.00 subject access fee, there might be a tendency to make greater use of enforced subject access than at present. This is another argument in favour of providing an effective sanction against enforced subject access.

As regards the voluntary sector, I am not persuaded that special arrangements need to be made. There is a practical difficulty of deciding which organisations would be entitled to lower cost vetting.

Question 7: Should individual application become the basis of a new system of vetting?

Response: I am not in favour of individual application being the basis of vetting checks. It could create a burden on individuals and lead to a confusion with subject access. It is better to have a procedure for vetting checks which is quite distinct from subject access so that enforced subject access requests can be recognised for what they are. The individual must, however, have the safeguard of seeing the record disclosed and having the right to challenge it (as, for example, exists under the Access to Medical Reports Act 1988).

I would like to see a procedure along the following lines:

1. A vetting request would be made direct by the employer to the vetting agency;

2. A copy of the request would be sent to the individual concerned, whose written consent would be sought beforehand;

3. The number of vetting checks made would be the minimum necessary – only the person to be offered an appointment should be vetted;

4. The response to the employer would be made only to a named person;

5. The employer would be required to have a written procedure which regulates the use of the information once received and ensures that it is only seen by the people who need to know, that it is only retained for as long as is necessary to make the decision about the appointment and that it is not further disclosed;

6. A copy of the information to be disclosed would be sent to the individual concerned

prior to disclosure to the employer, thereby giving the individual the opportunity to identify any problems with the information;

7. The individual concerned would have the right to challenge the information either direct with the employer or through the agency.

Whilst I have referred to "employers" in the suggested procedure it should, of course, apply to any organisations undertaking authorised vetting checks in other capacities eg licensing authorities.

Question 8: (a) Who should handle vetting enquiries? (b) Is there a role for a vetting agency and, if so, what should its functions be? (c) Should the vetting function be privatised?

Response: I am in favour of a vetting agency independent of the police. Indeed, this is the position which I took in my evidence to the Home Affairs Committee and to the Efficiency Scrutiny.

Such an agency would be in the position of having to make quasi public policy decisions or at least decisions on interpretation of public policy. For this reason it should be open to public scrutiny and its governing board should be representative and not be dominated by any particular interest.

Question 9: Would the exclusion of local record information from any and all categories of employment vetting significantly reduce the value of checks?

Response: I have no view on whether the exclusion of local record information would reduce the value of checks. This is perhaps something which could be answered in the light of the detailed examination referred to earlier. It would certainly be simpler from the administrative point of view to be able to confine the search to one source.

If it were established that for certain categories of checks local information would be valuable, it would be sensible for the vetting agency to act as a clearing house. Employers would make a request to the agency who would then direct the request to the appropriate local force and channel the response to the employer (and to the individual concerned).

Question 10: Is legislation desirable: (a) to set out those areas in which criminal record checks would be appropriate?; (b) to define what criminal record information might be released in various contexts?

Response: In my view, legislation is desirable to achieve both the objectives set out in Question 10. I accept however that it may not be possible to get all the detail into primary legislation. Some would need to be left for subsequent regulations and some left for interpretation (under guidelines established in legislation) by the vetting agency.

I raise again the issue of enforced subject access and repeat my view that this should be dealt with by legislation, making it a criminal offence for anyone to require an individual to exercise his right of access for that other's benefit. Reference has been made in the paper to the Draft EC Data Protection Directive which would give individuals the right to refuse to exercise their subject access rights under compulsion by a third party. This is a welcome step forward, but it is not clear how this would be implemented in practice and whether this would go far enough. I would be concerned if this were relied on as the means of dealing with the enforced subject access problem.

Statutory restrictions on other sources of an individual's criminal history may also be necessary.

Question 11: Is the current range of exceptions to the Rehabilitation of Offenders Act so wide as to undermine the Act's effectiveness? Should the exceptions be the same as

those areas of employment etc, which would also be subject to criminal record checks? Or should they be narrower and include only the most sensitive employment categories?

Response: I do not think it appropriate for me to express a view on the exceptions to the Rehabilitation of Offenders Act.

Question 12: Should a national vetting body, if one were to be established, be prepared to acquire information on the practice in some other countries with regard to criminal record checks, and investigate the possibility of reciprocal arrangements with some of those countries?

Response: It would be sensible for a national vetting agency to examine the practice in other countries and to investigate the possibility of reciprocal arrangements. It is important though that any such arrangements should preserve the safeguards for individuals which are mentioned in my response to Question 7.

The vetting agency could also examine the usefulness of certificates of good conduct in vetting people from overseas.

E J Howe
Data Protection Registrar
23 December 1993

Appendix 3

Calling Line Identification (CLI). Caller Display – Use of Captured Data

Note: This paper gives the Registrar's preliminary view.

1. By Caller Display we mean the facility for users of the telephone network which provides for the display and possible capture of the caller's number by the called party. Such a facility is currently under trial by British Telecom and is expected to be available to most users of the telephone network in the UK before the end of 1994.

2. Caller Display raises a number of data protection issues, some of which were addressed by the Data Protection Registrar in an Appendix to his Eighth Annual Report, June 1992 under the heading "Calling Line Identification". The Registrar concluded that the introduction of Caller Display without appropriate safeguards for the caller would be likely to contravene the First Data Protection Principle. This requires (inter alia) that personal data must be processed fairly. The safeguards must include a simple, free to use method of suppressing the display of the caller's number at his choice.

3. Concerns about protecting the privacy of the caller have been recognised by the network operators, and, when Caller Display is introduced nationally in the UK, the caller will be able to suppress the display of his number on a call-by-call basis by dialling the prefix 141. Suppression will also be possible for all calls made from a particular number.

4. Thus, the Data Protection Registrar is content that the data protection concerns which he raised in his Eighth Report are being addressed by the network operators. Discussions are continuing between the operators, OFTEL and the Registrar on the details of implementation.

5. However, the use of Caller Display once the service becomes available raises new data protection concerns which are outside the control of the network operators. The essence of the matter is that Caller Display allows not only the display but the capture of the caller's telephone number by the called party. If that number is subsequently held as personal data by the called party, the question arises: has it been obtained fairly?

6. It is a requirement of the First Data Protection Principle that information to be contained in personal data is obtained fairly. The Registrar's view is that this means that the source of the information should know who is to use the data and for what purpose or purposes the data are to be used or disclosed. If these matters are not obvious because of the nature of the transaction, they must be explained to the source before the information is given. This view has been supported by the Data Protection Tribunal in its recent decision regarding Innovations (Mail Order) Limited.

7. There are a number of reasons why the calling number might be retained by the

called party. These range from use by a private subscriber simply to return the call, to commercial use such as enhancing an existing customer database or establishing a new database.

8. The Registrar would accept that use of the captured number in direct connection with the original call by the called party is a use which the caller would reasonably expect. Such use could include the example above of returning a call if the called party had been unable to take the original call immediately. (In any event, in this case it is arguable that the information retained is not personal data.) Another such use, in a commercial context, would be to reference an existing customer database if the number were already held on it.

9. However, the Registrar considers that retaining the number and holding it as personal data if it were not already held as such is something which would not be obvious to the caller. In those circumstances, it is likely that the fair obtaining requirement of the First Principle would have been contravened by the called party if no explanation had been given to the caller.

10. In practice, it is difficult to see how the caller can be given such an explanation before he provides his number to the called party. By the time the call has been established, it is too late: the called party already has his number.

11. The only solution then is that the called party must seek the express consent of the caller to the retention of his number. If that consent is declined, the caller's number must not be held as personal data.

12. It is easy to envisage circumstances in which the calling number would be retained for purposes which are unconnected with the original call. An example would be to enhance a marketing database which is intended to be rented to other companies for their marketing purposes. The Registrar considers that to retain the number for such purposes without the express consent of the caller, would be likely to contravene the First Data Protection Principle.

13. However, the Registrar accepts that there may be uses arising from the original call (other than the obvious one of merely returning the call) for which it could be argued that retention without consent would not be unfair. As Caller Display is such a novel facility, no doubt novel and innovative uses of the captured number, which can not be foreseen at this stage, will be developed. The Registrar will be seeking discussions with appropriate representative bodies with a view to issuing more specific guidance.

14. In summary, the essence of the matter is that the caller's number may only be captured and held as personal data by the called party for purposes directly connected with the original call, unless the caller gives express consent to its subsequent use for other purposes. The Registrar is prepared to discuss with potential users of captured data whether the uses which they envisage fall into the category of not requiring consent.

Data Protection Registrar
27.4.94

Appendix 4

Smart Cards – Report of the Information and Privacy Commissioner, Ontario, Canada[1]

I am grateful to Tom Wright, the Ontario Information and Privacy Commissioner, for his agreement to produce the following extract from his report on smart cards. The extract outlines his proposed privacy protection requirements in respect of smart cards.

"Due to the nature of the technology, there is a need to go beyond statutory requirements to establish the following fundamental privacy protection requirements for all smart card applications:

— Smart card systems should be open and transparent to data subjects. They should know their inherent rights when using the card, what information the card contains, how it will be used, and what risks that use implies".

— Data subjects should have the right to participate in the determination of what personal information the card contains and who has access to it.

— Data subjects should have the right of access to and correction of information held about them on the card, as well as in any related databases.

— All uses and disclosures of information on the card should be subject to the prior and informed consent of the data subject.

— Where possible, individuals should be free to refuse the card without jeopardizing their access to the service involved. Similarly, holding a smart card should not confer benefits (other than perhaps enhanced service) unavailable to those who choose not to utilize a smart card.

— The full measure of security available through the technology should be used to prevent misuse or inadvertent access. This should include the use of PINS, authentication protocols, encryption, and the segregation of multi-use applications to prevent possible merging or matching of various databases. The use of smart cards to conduct computer matches or linkages should be restricted.

— Smart card technology should only be used by government organizations to enhance access to government information and services and not as an instrument of social control (eg. as a method of conducting surveillance or a means of creating computer profiles).

In addition, the standards or guidelines should require the preparation of a privacy impact statement prior to the approval of a new, or revision to an existing smart card application. Approval should be contingent upon a demonstration that privacy will be adequately protected. Such a step should be required prior to the introduction of any potentially privacy-intrusive technology.

---

1 Office of the Information and Privacy Commissioner/Ontario, April 1993.

Privacy impact statements should include, at a minimum, the following:

— a description of the proposed smart card application;

— a discussion of how the proposed application is in compliance with the Acts.

— an evaluation of the probable or potential effects that the proposed smart card application would have on the privacy of the data subjects and users;

— a discussion of what methods will be introduced to restore any lost degree of privacy should the introduction of a smart card application compromise existing levels of privacy afforded the data subjects;

— a description of all the personal information to be collected for the entire application, the manner of collection, the method of notification, and the reasons why that information is necessary and relevant;

— a description of the personal information to be held on the card and why;

— a listing of the proposed authorized users and what levels and/or types of access they would be provided;

— a description of the proposed procedure for data subjects to gain access to, and to correct their personal information, including a mechanism for appealing denial of access or correction;

— a description of the procedures to be used to ensure, as much as possible, the accuracy and timeliness of all personal information;

— a description of all the security measures to be used to ensure the protection of personal information and to restrict the possibility of unauthorized computer matches or linkages;

— a description of what previously unavailable/available personal information the proposed application would reveal or protect, make available or unavailable to any party;

— identification of the individual(s) responsible for the on-going assurance of security and privacy protection;

Smart cards can be used either to subvert informational privacy, or to preserve it. The choice is not driven by the nature of the technology, but rather by the priorities of the issuer – in this case, the government. To ensure that smart card technology does not negatively impact upon the information society, protection of privacy is not only a priority – it is a necessity."

Appendix 5

Research Results

In order to monitor attitudes and knowledge about data protection and related issues, 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 two classes – those results relating to members of the public and those relating to business establishments.

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

The tables show the main results of the research undertaken over the last three years. However, research has taken place annually since 1986. The full research results for the current and past years are available for study by interested parties.

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

(b) *Business Establishments* (Tables 10 to 13)

The tables show the main results of the research undertaken in the last three years. However, research has taken place in the first half of the year since 1986. The full research results for the current and past years are available for study by interested parties.

The surveys were 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.

The samples are representative of respective universes and weighted to reflect the profile of business establishments in terms of number of employees and type of industry.

(c) *Statistical Significance*

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

In calculating significance a design factor of 1.2 has been applied in recognition of the clustered nature of the sample in which sampling error will have been greater than for a pure random sample of the population, in which each individual had an equal opportunity of being selected.

Table 1

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

	1992		1993		1994
	%		%		%
Proportion saying the following are very important:					
Preventing crime on the streets	91	**	85		86
Improving standards of education	82	**	78		79
Protecting peoples rights to personal privacy	78	**	66		66
Unemployment	80		78	**	73
Inflation	66	**	46	**	53
Protecting freedom of speech	67	**	53		57
Making sure women have equal rights	61		57		53
Protecting the rights of minority groups	40		40		36

** = statistically significant.

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.

	1992	1993	1994
	%	%	%
Proportion saying the following are of most concern:			
Keeping personal information/ details private	76	73	71
Protecting the privacy of your own home/property	78	79 **	75
Being able to do what I want in my own home	64	66	62
People telling me what to do/ interfering with my life	58	58	56
Organisations building up files of information about me	52	49	53
Maintaining freedom of movement/speech/ religion	50	53	56
Stopping unwanted mail/telephone calls/selling	51	49	47
Individuals prying into my business	52	53	53

** statistically significant

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.

	1992		1993	1994
	%		%	%
Very concerned	39	**	33	36
Quite concerned	34		35	36
Neither/Nor	8		11	9
Not very concerned	12		15	13
Not at all concerned	5		5	5

** = statistically significant

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.

	1992		1993		1994
	%		%		%
Proportion saying very or quite concerned:					
Your savings	77		75		74
How much you earn	72		70		68
Court judgements	67		67	**	62
Credit ratings	68		65		63
Your visitors	60		59		59
Medical history	61		62		64
Education and job history	43		40		38
What you buy	39	**	32		30
Membership of clubs	27	**	22		25
Your TV viewing	12		12		13
What papers you read	14		15		14
Your age	15		15		13

** = statistically significant

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.

	1992		1993		1994
	%		%		%
Doctors and the NHS					
Satisfied	92		92	**	88
Not satisfied	5		3		5
Banks and building societies					
Satisfied	78		75		74
Not satisfied	13		16		18
Employers					
Satisfied	74		72		69
Not satisfied	11		11		13
Police					
Satisfied	72	**	78	**	72
Not satisfied	15		12		16
Inland Revenue					
Satisfied	68		68		67
Not satisfied	17		15		18
Schools and colleges					
Satisfied	66		70	**	63
Not satisfied	12		7		10
DHSS					
Satisfied	63		65		61
Not satisfied	16		15	**	20
Shops and stores					
Satisfied	36		32		35
Not satisfied	41		40		36
Credit reference agencies					
Satisfied	25		30		29
Not satisfied	49		41		45
Mail order companies					
Satisfied	23		23		22
Not satisfied	57		54		51

** = statistically significant:

Table 6

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

	1992	1993	1994
	%	%	%
Proportion saying the following rights are very important:			
To correct errors in information about yourself	83	84	83
To know what the information about you is being used for	80	80	81
To be told who the information about you is being passed to	83	83	81
To be told where the information about you came from	77	80	77
To see what information is held about you	77	79	77
To have yourself removed from lists or files	78	75	71
To add things to the information about yourself	68	69	65

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.

	1992		1993		1994
	%		%		%
Aware that there is a law concerning rights about information kept on individuals	22		20		24
Spontaneous awareness of the Data Protection Act	9		8		11
Prompted awareness of the Data Protection Act:					
Definitely heard of	20		19		23
Think so	9		11		13
TOTAL AWARENESS OF THE DATA PROTECTION ACT	38		38	**	47
Made use of the Data Protection Act	3		4		4
Think the Data Protection Act is very useful	67	**	61		57
Semi-prompted awareness of the Data Protection Registrar#	34		35	**	45
TOTAL AWARENESS OF DATA PROTECTION*	51		53	**	64

= Chosen from a list of likely sounding titles, eg. Home Secretary, Privacy Commissioner, etc.

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

** = statistically significant

Comment

Significant increases in awareness of the Act, the Registrar and total awareness of data protection.

Table 8

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

	1992	1993	1994
Base: all aware of the Data Protection Act	384	381	470
	%	%	%
Right to find out what information is held about you	16	15	13
Protecting your rights about what information is kept on you	21	19	23
Firms need to register	6	7	8
Have to pay	1	2	3
Able to correct wrong information	7	3	6
Only see computer records	2	1	3

Table 9

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

	1992	1993	1994
Base: all aware of the Data Protection Act	384	381	470
	%	%	%
Proportion saying the Data Protection Act performs the following functions:			
Enforcing your right to see information kept about you	63	62	65
Enforcing your right to correct information kept about you	62	61	66
Controlling information that can be kept on you	56	48	57
Monitoring all personal information on paper as well as on computer	35	40	34
Stopping organisations passing information about you to others	43	44	44
Making people who misuse information liable to imprisonment	40	35	40
Providing compensation if you are harmed by the misuse of information	29	28	29

Table 10

Businesses were asked about their use of computers and computer records.

	1992	1993	1994
Use computer/computer bureau			
Small Companies (fewer than 50 employees)	50	53	54
Large Companies (50+ employees)	100	100	100
Personal records on computer*			
Small Companies (fewer than 50 employees)	46	51	50
Large Companies (50+ employees)	100	100	100

* = Base: all who use computers

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.

	1992	1993		1994
Prompted Awareness of the Data Protection Act:				
Small Companies (fewer than 50 employees)	88	87		86
Large Companies (50+ employees)	97	97		97
Semi-prompted awareness of the Data Protection Registrar*				
Small Companies (fewer than 50 employees)	58	54	**	46
Large Companies (50+ employees)	72	75	**	61

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

** = statistically significant

Comments

Significant decline in awareness of the Data Protection Registrar among both small and large establishments.

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).

	1992	1993		1994
Aware of need to register				
Small Companies (fewer than 50 employees)	62	59		60
Large Companies (50+ employees)	85	85		80
Aware of data users' obligations				
Small Companies (fewer than 50 employees)	29	29		24
Large Companies (50+ employees)	45	56	**	45

** = statistically significant

Comment:
Significant fall of awareness of data users obligations among large companies.

Table 13

All businesses holding personal records on computer were asked questions to ascertain their awareness that the Act conferred rights on individuals.

	1992	1993	1994
Aware of individuals' rights			
Small Companies (fewer than 50 employees)	50	46	43
Large Companies (50+ employees)	75	75	72

Comments
Further questions asked about understanding of individuals' rights in detail revealed a significant drop in small data users' awareness of an individual's right to see information (81% to 64%). Amongst large data users, there was a significant drop in awareness of an individual's right to correct information (29% to 18%). However, amongst both small and large data users there were significant increases (albeit from low bases) in mentions of the right to confidentiality. This last change may be due to the Registrar's publishing of a view on the law of confidentiality in respect of financial information.

Appendix 6

Extract from the Summary and Conclusions of "Data Protection Controls and Safeguards". Report by the Comptroller and Auditor General, 20 August 1993.

"In the light of these findings the National Audit Office consider that, to improve and strengthen the protection of the public, the Data Protection Registrar should:

— Renew and redirect efforts to increase the number of data users registered under the Act;

— strengthen controls over those applying to register, with sample checks to ensure they are following good practice;

— review the nature and current level of the risks to the public by failures by data users to follow required controls and good practice;

— produce and implement a strategy for the direct monitoring of compliance with good practice;

— check in all cases to ensure that formal supervisory notices are complied with;

— take steps to improve significantly what people know about the Data Protection Act, and their rights under it, and how any complaints should be pursued;

— make the Data Protection Register more readily available to the public.

The National Audit Office believes that actioning these recommendations could materially assist the Registrar in carrying out his task. But there are constraints limiting the implementation of the recommendations. First, there are limitations on the Registrar's powers and functions under the Data Protection Act. But although there may be difficulties in securing any necessary changes in the short-term, preparing for revised legislation that would follow the adoption of the Data Protection Directive would provide a good opportunity to review the present provisions and identify necessary changes. Second, this report is concerned primarily with what the Registrar is doing and might do to meet statutory and other requirements. It is for the Registrar to assess any extra resources required, taking into account whether different use of existing resources might be possible; and ultimately for the Home Office to determine the level of grant in aid which is made available, having regard to wider competing demands."

Appendix 7

Data Protection Registrar

Statement Of Account For The Year Ended 31 March 1994

Data Protection Act 1984

FOREWORD

Background Information

1. The Registrar was appointed on 20 September 1984 under Section 3(2) of the Data Protection Act 1984.

2. Under paragraph 7(1)(b) of Schedule 2 to the Data Protection Act 1984 the Registrar is required to prepare a statement of account for each financial year in the form and on the basis directed by the Secretary of State, with the consent of the Treasury. The account is prepared on a cash basis and must properly present the receipts and payments for the financial year and the balances held at the year end.

3. As the senior full time official, the Registrar carries the responsibilities of an Accounting Officer. His relevant responsibilities as Accounting Officer, including his responsibility for the propriety and regularity of the public finances for which he is answerable and for the keeping of proper records, are set out in the Non-Departmental Public Bodies' Accounting Officer Memorandum.

Review of Activities

4. The purposes of the Act are to:

   — make the nature and use of personal data in computing systems open to public scrutiny (through a public register and by enabling individuals to obtain details of information about themselves);

   — ensure good practice in the use, processing and protection of personal data in computing systems (through promoting and enforcing the Data Protection Principles); and

   — allow individuals to claim compensation for damage and any associated distress arising from lack of security surrounding personal data which concern them or from inaccuracies in such data.

5. Activities in respect of the European Union continue to extend. These cover the Draft Directive on Data Protection and activities in respect of customs and police collaboration. There is an increasing necessity for discussion and agreement with other Data Protection Commissioners.

   The requirements for lawfulness in the Data Protection Principles have led to

consideration of the effect of the law of confidence in regard to the use and disclosure of financial and medical information.

The Data Protection Tribunal confirmed the views of the Registrar in an enforcement action about the fair obtaining of information for direct marketing.

The latest research suggests that the number of individuals aware of the Data Protection Act or the Data Protection Registrar has increased significantly from 53% in 1993 to 64% in 1994.

Events since the end of the Financial Year

The Tenth Annual Report of the Data Protection Registrar will be laid before Parliament on 5 July 1994. This gives fuller details of activities.

E.J. HOWE CBE
Data Protection Registrar

13 June 1994

STATEMENT OF RECEIPTS AND PAYMENTS ACCOUNT FOR THE YEAR ENDED 31 MARCH 1994

	Notes		1993/94		1992/93
		£	£	£	£
H.M. Grants received	2	3,429,000		3,744,169	
Operating receipts	3	4,415,407	7,844,407	7,726,669	11,470,838
Salaries and Wages	8	1,550,433		1,537,864	
Other operating payments	4	1,843,780	3,394,213	2,127,335	3,665,199
Surplus from operations			4,450,194		7,805,639
Other Receipts	5	78,450		115,577	
Other Payments	5	54,565	23,885	58,256	57,121
Surplus for Year			4,474,079		7,862,760
Appropriations	6		4,573,922		7,628,141
Excess of receipts over payments (payments over receipts) for the year			(99,843)		234,619

STATEMENT OF BALANCES AS AT 31 MARCH 1994

	Note	1994	1993
		£	£
Balance at beginning of year		258,429	23,810
Excess of receipts over payments (payments over receipts) for the year		(99,843)	234,619
	7	158,586	258,429

The Notes on pages 91 and 92 form part of this Account.

Notes to the Statement

		1993/94	1992/93
		£	£
1.	This account is drawn up in a form directed by the Secretary of State, and approved by the Treasury.		
2.	HMG Grants Received.		
	Grants received from Class VIII Vote 3 Subhead L6 1993-94	3,429,000	3,744,169
3.	Operating Receipts		
	Receipts from registration fees	4,415,407	7,726,669
4.	Other Operating Payments		
	Rents & rates	356,921	265,590
	Maintenance, cleaning, heating & lighting	74,125	58,556
	Office supplies, printing, stationery	65,428	77,320
	Carriage & telephones	96,830	97,406
	Travel & subsistence	125,024	124,708
	Staff recruitment	2,429	3,648
	Specialist assistance	5,553	2,554
	Public relations	411,730	649,902
	Legal costs	54,095	67,754
	Staff training/health & safety	34,571	27,102
	Computer bureau	419,173	491,731
	Vehicle expenses	1,136	1,361
	Audit fee	6,300	6,050
	VAT	190,465	253,653
		1,843,780	2,127,335
5.	Other Receipts/Payments		
	Receipts		
	Pension contributions/transfers	24,818	39,480
	Bank interest	40,729	61,103
	Other interest	-	200
	Speakers' fees	250	476
	Sale of Goods	83	2,037
	Legal Costs recovered	12,412	12,081
	Other Income	158	-
		78,450	115,377
	Payments		
	Purchase of computer hardware/software	36,620	27,013
	Purchase of furniture & other office equipment	9,895	22,473
	VAT	8,050	8,770
		54,565	58,256
6.	Appropriations Amounts surrendered to the Consolidated Fund via the Home Office during the year		
	Registration fees	4,494,714	7,512,764
	Other	79,208	115,377
		4,573,922	7,628,141

		1993/94	1992/93
		£	£
7.	Balance at Year End		
	Cash at bank	158,391	258,106
	Cash held at offices	195	323
		158,586	258,429
8.	Salaries and Employees		
	(a) The salary of the Registrar is paid from the Consolidated Fund and is not therefore included in this account.		
	(b) Corporate Managers		
	The emoluments of Corporate Managers fell within the following ranges:	No.	No.
	£		
	25,001 – 30,000	1	0
	30,001 – 35,000	0	0
	35,001 – 40,000	1	1
	40,001 – 45,000	1	2
	45,001 – 50,000	1	0
(c)	Staff Costs		
	Salaries and Wages	1,436,162	1,374,919
	Social Security Costs	108,216	97,982
	Pension Costs	6,055	64,963
		1,550,433	1,537,864
	The average number of persons employed by the Registrar during the year was as follows:		
	Category	No.	No.
	Corporate Management	4	3
	Senior Staff	5	6
	Other Staff	84	86
	Occasional Casuals (full-time equivalent)	4	4
9.	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.		

E.J. HOWE, CBE
DATA PROTECTION REGISTRAR

13 JUNE 1994

The Certificate of the Comptroller and Auditor General to the Houses of Parliament

I have audited the financial statements on pages 90 to 92 which have been prepared in a form directed by the Secretary of State for the Home Department and approved by Treasury.

Respective responsibilities of the Registrar and the Auditors

As described on page 88 the Registrar is responsible for the preparation of the financial statements. It is my responsibility to form an independent opinion, based on my audit, on those statements and to report my opinion to you.

Basis of Opinion

I certify that I have examined the financial statements referred to above in accordance with the Data Protection Act 1984 and the National Audit Office auditing standards, which include relevant Auditing Standards issued by the Auditing Practices Board. An audit includes an examination, on a test basis, of evidence relevant to the amounts and disclosures in the financial statements. It also includes an assessment of the significant judgements made by the Registrar in the preparation of the financial statements, and of whether the accounting policies are appropriate to the circumstances of the Data Protection Registrar, consistently applied and adequately disclosed.

I planned and performed my audit so as to obtain all the information and explanations which I considered necessary in order to provide me with sufficient evidence to give reasonable assurance that the financial statements are free from material mis-statement, whether caused by fraud or other irregularity or error. In forming my opinion I also evaluated the overall adequacy of the presentation of information in the financial statements.

Opinion

In my opinion the financial statements properly present the receipts and payments of the Data Protection Registrar for the year ended 31 March 1994 and have been properly prepared in accordance with the Data Protection Act 1984, as directed by the Secretary of State with the approval of Treasury.

I have no observations to make on these financial statements.

John Bourn
Comptroller and Auditor General

Date 22 June 1994

National Audit Office
157–197 Buckingham Palace Road
Victoria
London SW1W 9SP

Printed in the United Kingdom for HMSO
Dd 5062717 5/94 C14 T3968 254/404

HMSO publications are available from:

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

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

HMSO's Accredited Agents
(see Yellow Pages)

and through good booksellers

ISBN 0-10-245394-
9 780102 45394