

Information Commissioner

Annual report and accounts for the year ending 31 March 2003

July 2003

Presented to Parliament pursuant to Section 52(1) and
Schedule 5 paragraph 10(2) of the Data Protection Act 1998 and
Section 49(1) of the Freedom of Information Act 2000.

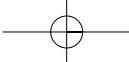
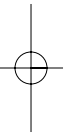
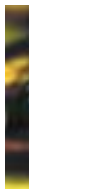
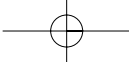
Ordered by the House of Commons to be printed 15 July 2003

London: The Stationery Office

Price: £20.50

HC727



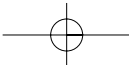
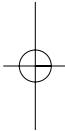
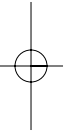
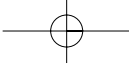


Contents



Commissioner's foreword	6
Chapter 1: Review of the year	10
Chapter 2: Some challenges we face	35
A surveillance society	35
Enforced subject access	36
Telecommunications issues	37
Chapter 3: The year ahead	40
Information Commissioner's Accounts for the year ended 31 March 2003	43
Appendix:	
Developments in Jurisprudence	70
Financial Matters	91
Output Measures and Performance Indicators	94
Our Annual Caseload	96

Note: The main body of this report outlines the main issues and developments of the office during the year. Although most figures relate to the year ending 31 March 2003, the report includes references to the developments which have taken place between the year-end and publication.



Our mission



We shall develop respect for the private lives of individuals and encourage the openness and accountability of public authorities:

- by promoting good information handling practice and enforcing data protection and freedom of information legislation; and
- by seeking to influence national and international thinking on privacy and on information access issues.



Management Board (left to right):

Graham Smith, *Deputy Commissioner*; Francis Aldhouse, *Deputy Commissioner*; Richard Thomas, *Information Commissioner*; Nicholas Tyler, *Legal Adviser*; Helen Corkery, *Marketing and Communications Director*; Mike Duffy, *Director of Personnel and Finance*.

Commissioner's foreword



Protection. Information. Freedom. The heady vocabulary of my remit as the new Information Commissioner brings a weighty challenge of responsibility. It involves a direct influence on the kind of society we live in. How should the balance be drawn between respect for privacy and the fight against crime? How can people discover a great deal more about what public bodies are doing in their name and which may affect their lives – without creating a goldfish bowl where good government becomes impossible?

Accountability is another key word. It is imperative – for both data protection and freedom of information – that no-one should be in any doubt about my independence. I have considerable autonomy. I have an extensive range of statutory duties and powers. My decisions and activities make a real difference to the behaviour of public and private organisations and their impact on individuals. I spend public money. All of this – and much else – means that I and my staff must be fully accountable. This Annual Report is one of the main instruments of that accountability.

As the new Information Commissioner – just seven months into a five year term – my first Annual Report must look backwards and forwards. I can claim little credit for the bulk of this report, which sets out the activities and achievements of my office over the last year. But this foreword provides me with the opportunity, indeed the responsibility, to outline my initial vision of the future.

"Elizabeth France will be a hard act to follow," was a refrain I heard many times after my appointment was announced in mid-2002. That truth was demonstrated at the International Data Protection conference which Elizabeth co-hosted in Cardiff in September, shortly before her departure. The strong respect, and affection, of the international and domestic data protection and privacy community was palpable on that occasion. The truth has been more than confirmed since I took over in December. She has bequeathed a healthy, vibrant

organisation – mature as one of the world's leading data protection authorities and enthusiastic at the prospect of making a reality of freedom of information. My deputies, Francis Aldhouse and Graham Smith, deserve special gratitude for keeping the office well on course during the inter regnum.

Despite such changes of leadership, it is remarkable how much has been achieved over the past year. The profile has probably never been higher. We have not avoided controversy. We are involved with an astonishing range of public policy issues – straddling health, social services, transport, education, marketing, telecoms, financial services, law enforcement and many other areas. We have developed and advanced our position by reference to clear principles. In a world of rapid change – political, social, economic, and technological – it is vital that we articulate the values of personal privacy and public openness. These values cannot simply be abandoned in the face of threats – whether from terrorism, serious crime, international instability or anti-social conduct on our streets. Nor can these values simply be abandoned against claims of progress and opportunity – whether widespread data sharing or intrusive telephone marketing in the name of improved customer service or excessive DNA profiling in the name of crime detection. Equally, the values of privacy and openness are not absolutes. Both require delicate and proportionate balances to be drawn in the face of both threat and opportunity.

This has been the approach which we have adopted on such issues as retention of telecoms and other communication data, access to such information, monitoring and surveillance in the workplace and in public places and access to passenger reservation information. Perhaps the most prominent – ironically the same was true in Elizabeth France's first annual report eight years ago – was my concern to ensure that strong safeguards are engineered into any scheme of universal entitlement or ID cards to ensure compliance with data protection requirements.

Much has also been achieved with our operational activities, which account for the bulk of our resources. I have been impressed with the thoroughness, know-how and courtesy with which my staff deal with thousands of enquiries, many involving a formal request for an assessment, some from troubled people. Likewise, data controllers are painstakingly helped to achieve compliance with the law so that enforcement action is only taken where really necessary. We run imaginative and well-targeted campaigns to raise individual and organisational awareness. With a lengthy implementation timescale, our freedom of information work has yet to take off. But we have already approved large numbers of freedom of information publication schemes, have negotiated model schemes with leading representative organisations and are developing detailed plans to deal with a new caseload which is unpredictable in quantity, but guaranteed to be difficult and sensitive.

Foreword

Through all of this, we have faced internal challenges. The Office's change programme, introducing a major up-grading of our ICT infrastructure and case management systems, is bringing the best out of the organisation - a determination to achieve real improvements with minimum disruption. The activities of the "bogus" data protection agencies - impersonating my office and conning thousands of organisations about notification requirements - have placed heavy burdens upon my front-line staff and caused difficulties and delays for those who want to contact us on other matters.

Where next? data protection and freedom of information are still sometimes seen as novel, controversial and threatening concepts. They will assume concrete shape in many unexpected ways. The complex and over-prescriptive legal framework does not help. It is not realistic to expect changes to the Data Protection Directive or the 1998 Act in the short term, but I am launching a project to identify the scope for simplifying data protection compliance, without damaging effectiveness. I want to explore, in particular, what might be put in place swiftly through secondary legislation or changes of enforcement policy.

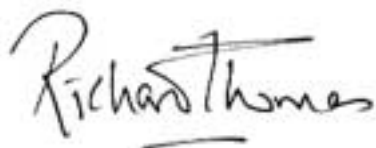
My central challenge, however, must be to deploy a strategic approach which will bring about a culture - in both public and private sectors - where data protection and freedom of information are seen as natural, beneficial and - ultimately - essential working disciplines. This will not be achieved quickly. My staff and I will need carrots and sticks, but the emphasis must be on persuasion, incentive and self-interest. We need legal sanctions, but will have failed if their use - to force people to do things they do not believe to be sensible - becomes the norm. Despite the daunting nature of the legislation, the underlying themes are straightforward. Which organisation wants to hold information that is inaccurate, out of date, or insecure? What body serving the public wants to generate suspicion and distrust through unnecessary secrecy?

The future demands a hand on the tiller, rather than any major changes of tack. Our immediate priorities are clear. We need to give more attention to freedom of information to ensure we are as ready as possible for January 2005 when the new Right to Know becomes fully operational. We will be establishing our regional offices in Scotland, Wales and Northern Ireland and a small pied-a-terre in London. Across all parts of the organisation, we must be proactive, good at communicating and confident in our powers of persuasion. We must ensure that we do not take an over-zealous approach or impose excessive burdens. Above all, we must be effective and this will mean targeting concerns - not necessarily those generating the most complaints - where the detriment is greatest or the public interest most acute.

In the autumn, we will be conducting, with external input, a comprehensive review of our aims and objectives to ensure that we are doing the right things, as well as doing things right. Following a top-level corporate governance review, I am also putting in place a new Management Board, with non-executive members to share with me and my senior staff the task of setting our strategic direction and ensuring that we achieve worthwhile results.

I am optimistic about the benefits of these improvements to our corporate planning and governance. My own background – ranging across public/private and consumer/supplier boundaries – is varied and it should surprise no-one that I attach considerable weight to clarity of purpose, objectivity and cross-fertilisation. A strengthened Management Board, coupled with revitalised corporate plans, should help us to become more outward-looking, see our functions within context, improve our effectiveness and strike the right balance amongst many competing public interests.

The challenges of the last year have been substantial and my staff have risen to these. The challenges for the year ahead appear equally formidable. Equipping ourselves with the right strategic and organisational framework will ensure that we continue to meet these and the challenge of weaving data protection and freedom of information into the fabric of society.



Richard Thomas, **Information Commissioner**

RICHARD THOMAS:

Richard Thomas took up the role of Information Commissioner in December 2002.

Richard's career includes:

- 1992-2002: Director of Public Policy at Clifford Chance (International Law Firm)
- 1986-1992: Director of Consumer Affairs at the Office of Fair Trading
- 1979-1986: Legal Officer and Head of Public Affairs at the National Consumer Council
- 1974-1979: Solicitor with the Citizens Advice Bureau Legal Services
- 1971-1974: Freshfields

Richard was previously a non-executive Director of the Financial Ombudsman Service and a member of the Independent Television Commission Advertising Advisory Committee.

Chapter 1:

Review of the year



As with previous Annual Reports, we have reviewed the year according to the Office's overarching aims and key objectives.

1) We will aim to ensure that the statutory duties placed upon us are met. To do this efficiently and effectively, we aim to be an organisation responsive to change and ready to manage risk in a way which allows the resources available to us to be best used.

Corporate planning

The considerable, and increasing, demands that have been placed on the Office during the period under review have caused us to look closely at our existing resources and how we can best use them. The challenges have been great. For example, we currently handle some 12,000 requests yearly from members of the public to assess whether the Data Protection Act is being complied with. We deal with many thousands of written requests from businesses and other record holders for advice about how best to comply with the law. In the period under review our enquiry line dealt with nearly 60,000 telephone enquiries, often difficult or complex ones. Although we are satisfied that we generally provide a good service, we intend to improve our service standards across the board.

In response to the pressures described above, we are in the process of reviewing all aspects of the way our Office is run. This involves looking, for example, at staffing issues and at the way we handle information within our organisation. Most importantly, we are reviewing how we deliver our services to the considerable numbers of individuals and businesses who, quite rightly, expect prompt, clear, responses to their enquiries about how to comply with the potentially complex pieces of law we are responsible for promoting compliance with.

Our corporate strategy for the future will focus on the external and internal challenges we face over the next three years and beyond. It sets out our direction and defines what we need or want to do and what sort of organisation we want to be. Dominating all our plans is the need to ensure that our priorities address the major challenges we face:

Challenges	Priorities
Implementation of Freedom of Information Act and other access laws.	Developing from a mature data protection organisation into the champion of both public openness and personal privacy.
Rising public concern over data protection issues.	Maximising our effectiveness and influence: <ul style="list-style-type: none">• more proactive;• influential profile;
Rapid changes – technology, law, policy, and public concerns.	<ul style="list-style-type: none">• strong at communicating;• successful promotion of good practice; and• enforcement targeted on mischief causing real detriment.
Modernising government agenda.	Enlarging/modernising our office: <ul style="list-style-type: none">• successful Change Programme;• Multi-site operation;• improved governance, structures and systems;• improved knowledge management;• useful service delivery targets and other ways to be sure we are succeeding;• ensuring our staff achieve their full potential; and• accommodation needs.
Growth of international activity.	Initiating and responding to major policy initiatives.
How best can we make a difference?	Getting the best from our international work.

Case Study

BREACH: Security

An individual made a complaint against a debt collection company which, in the process of trying to collect the debt, disclosed information about the complainant's account to members of his family. The information disclosed included details of how much the individual owed. It appeared unlikely that the processing concerned had been in compliance with the Act and in particular appeared to contravene the seventh data protection principle. Although the debt collecting company stated that staff undergo induction training on data protection when they first join the company, the recommendation was made that debt collectors should undertake regular annual training to ensure future compliance.

The corporate planning process has involved establishing a business plan for the one-year period 2003-4. This sets out the planned programme for each team and has been agreed with the person responsible for leading the team. The overall plan records all the main work we will be carrying out over the year up to end-March 2004. We have also set out a Corporate Plan for the period 2003-6. This is a longer term, less detailed, plan. It sets out the major challenges we face as an organisation, and the main priorities which should guide our activities. There will be a major review of this longer-term Corporate Plan during the autumn so that there is likely to be a fresh approach for the three years from April 2004.

The new-look Business Plan for the current year will enable us to link objectives to particular areas of work. With this in mind, we are therefore also making some changes to revitalise the staff development review process which most people have come to feel has become a little dated over the last few years. The aims of these changes are to make clear links between individual objectives and those of the Office and to give individuals a greater opportunity to contribute to their own review process.

Staffing

The number of established staff in the Office increased by 30 over the year, taking the end of year figure to 197. In addition, we had 16 staff on temporary or agency contracts, filling posts whilst the competitions for established appointments were completed. This last year increase means that established numbers have increased by 53.9% (MO) over the last two financial years. This build-up is in line with our projections for staffing needs in readiness for our growing Freedom of Information responsibilities. These will come fully into force in January 2005 with the introduction of individual access rights to information held by public authorities. We have much work to do in the interim in terms of approving publication schemes, working with bodies on their responsibilities and planning for the introduction of individual rights.

Three of the more significant appointments during the year were those of the Assistant Commissioners, who will set up and manage the regional offices to be established in Scotland, Wales and Northern Ireland. It was our first experience of recruiting staff for offices away from Wilmslow, and it was encouraging to generate so much interest and to receive so many high quality applications.

The three Assistant Commissioners for these satellite offices will be based mainly in Wilmslow for the first six months of their appointments, building up their knowledge of the legislation and finalising project plans to cover the establishment of their respective offices. Their short term accommodation in

the Wilmslow offices has increased the accommodation pressures, as we expected during this build-up period. We have used professional space planners to ensure that we are making the best use of the space available to us. Towards the end of the year, we initiated the project to determine our longer term space needs and to identify appropriate accommodation.

We were delighted to have our Equality Scheme, produced as part of our responsibilities under section 75 of the Northern Ireland Act 1999, approved by the Northern Ireland Equality Commission. The Scheme will undergo a complete review in readiness for our establishing an actual presence in Northern Ireland. In the meantime, we have carried out training for relevant staff on the specific requirements within Northern Ireland. We plan to include awareness of these obligations within general diversity training for all staff. That general training is in line with other innovations put in place during the year with regard to monitoring under Commission for Racial Equality requirements.

The appointment of a full-time training officer has meant that we have been able to concentrate much more on the development of staff, which has been particularly important given our rapid growth. The aim has been to ensure that staff are able to become effective in as short a time as possible after appointment. Although training is always important, it will be a particularly critical issue for us in what will be a further year of growth and change.

In recognition of our expansion and increased responsibilities, we were able to carry out some changes to senior pay as part of this year's pay settlement. Restrictions in the years since pay was delegated have meant that we have been unable to keep pace with salary developments elsewhere, particularly at those senior levels. This coming year, following a full Equal Pay Audit, which we have recently commissioned, we shall be carrying out a market review of the reward package for staff at other levels. The improvements we have secured in recent years have really assisted recruitment in what is still a very competitive local market. The steps planned will help to ensure that we are able to retain and attract suitable staff to continue the growth through to 2005.

Information Management

Over the last two financial years the Office has been in receipt of a one off investment towards the Modernising Government Programme. This has been invested in a brand new Information and Communications Technology (ICT) infrastructure to provide the platform for contemporary professional support tools and business applications to support case management, electronic document and records management, knowledge management and electronic

Case Study

BREACH: Unfair processing

An employer believed a member of staff was claiming more hours than he was working.

The employer used an organisation to conduct covert surveillance of the employee and subsequently the employee was dismissed.

The employee made a request for assessment to the Information Commissioner.

The employer believed they could rely on section 29(1), the crime and taxation exemption, in respect of the covert surveillance.

Although potentially the employee may have committed a criminal offence of obtaining property by deception, it was unlikely that the employer could rely on Section 29 (1) because covert monitoring can only be justified where complying with certain provisions of the Data Protection Act would be likely to prejudice the prevention or detection of crime or certain other purposes. It did not appear that the data controller had conducted a considered and realistic assessment of whether this was the case.

Information Commissioner – Annual Report and Accounts 2003

service delivery. The project to implement the new ICT infrastructure was completed in March 2003.

The Commissioner's new infrastructure project included an aim to make direct e-mail and internet access available to every member of staff. In order to bring this about in as secure a manner as possible and to provide a secure basis for the computerisation of other work processes in the office, a decision was made to apply for accreditation to the Government Secure Intranet (GSI). This is an IT network covering Government Departments and public bodies. It gives secure internet and e-mail access and the ability to transfer files safely between members. In order to gain accreditation we had to provide assurances to the accreditation panel that specific security measures were in place. A project was set up to consider the general security environment, as well as to ensure that appropriate technical measures were in place to protect the computer system. Evidence that those measures were in place was provided to GSI in December 2002, and the Commissioner achieved accreditation in January 2003. A statement of compliance with the GSI Community Security Policy has to be provided every six months and a full review carried out biannually.

An e-Government framework has been designed in conjunction with Fujitsu Services, our Information Services provider. This will be capable of supporting the whole of the office's business processes. Once implemented it will meet the government's targets for electronic document and records management, and for electronic service delivery. The application is built around the Meridio product set for electronic document and records management and Customer Application Solution (CAS) for workflow. It is currently undertaking user acceptance testing and is due to be rolled out during the summer of 2003. There are considerable challenges ahead to embed new ways of working into our organisation.

To address the changes ahead we have invested in a new training facility which can simulate our working environment. Our staff will have the advantage of becoming familiar with the new application in a safe environment away from the live network.

Some investment has been made to underpin the work carried out by our support teams. The software Computers in Personnel has been procured and will be implemented during 2003. The telephony switchboard has been upgraded and a real time reporting package will provide information to enable us to handle our calls more effectively.

Much of the work of the programme has been to establish a foundation for future development activity, for example in the area of knowledge management. In the year ahead we will be reviewing our IS strategy to ensure that it is aligned with ICO's business objectives. We will be establishing new ways of working and reviewing the impact of the changes we have made.

Website Redevelopment

In the light of internal electronic developments and changes to our communications throughout the organisation, the opportunity presented itself to update our external online presence. In order to achieve our goal, a project plan was produced and a selection process was undertaken using agencies with a website / marketing mix bias.

'Amaze' was appointed to undertake our website redevelopment project. Given the short timescale of the project, just four months, an internal working group consisting of ICO stakeholders was set up to help deliver the contents of the end product.

The new site will be supported by a content management system which will be compatible with the key elements of our ICT infrastructure. Content will be managed using metadata that complies with Public Records Office requirements. It matches that used to set up our in-house document and records management systems. This ensures that compatibility with our document and records management systems will be secured, should we decide to bring the system in-house. The design of the site is compliant with all current accessibility guidelines. The site is currently hosted by a third party, but the content management system will allow us to update the site directly.

Work conducted focused on developing the core functionality of the site. The new site will eventually offer a number of new features:

- an interface to our electronic service delivery channels, providing online notification, requests for assessment, publication scheme submission and enquiries;
- an interface with the current online register of data controllers;



Case Study

BREACH: Unfair Processing

A data controller was setting up procedures for in-house training of its customer-facing staff. To help in this, they needed to find an example upon which to base their new procedures. The example used was of an existing staff member who had recently had occasion to use the company's facilities as a customer.

The staff member was unaware that this had taken place, and only realised what had happened when other employees began referring to his experience.

The data subject requested that the Information Commissioner make an assessment. They assessed that the data controller was unlikely to have complied with the Act and recommended appropriate changes to the procedures involved. The data controller removed the individual's data and replaced it with a theoretical example not linked to any actual person. They also put in place procedures to safeguard future use of real-world data in their training.

- a 'have your say' facility, offering a means by which we can invite feedback on drafts for consultation and other areas of work in a structured way;
- e-mail alerts (subscriptions) to all or any part of the site, to ensure that visitors are kept up to date with changes and additions to the site;
- document archives, allowing visitors to search for past versions, news releases and other archived materials;
- education and training and media services centres;
- advanced search options for those who know what they are looking for;
- a range of 'expandable movies' to assist visitors who are not familiar with our role or the legislation with an accessible overview of their rights and obligations;
- a list of latest site-wide news and events which is automatically updated as new items are introduced to the site;
- a range of 'Quick links' allowing visitors to go straight to important site sections and/or content; and
- lists of recently published items and current issues.

The new site has been future proofed for a more sophisticated workflow and automated e-mail routing. The planned go-live date is July.

One of the projects that had to be undertaken was the creation of five expandable movies, which are used as an animated narrative of key everyday questions asked by enquirers for example: What does the ICO do? In order to build such a 'movie' the following process had to be undertaken;

- 1 Stakeholders identified
- 2 Structure of the text was defined and agreed
- 3 Copy was written by stakeholders
- 4 Copy was edited by Marketing
- 5 Copy was edited by Amaze
- 6 Copy was agreed
- 7 Design and structure demonstrated and reviewed online
- 8 First complete draft incorporating copy tested and reviewed online
- 9 Completion agreed

Notification

The maintenance of the statutory register of data controllers has continued to be a significant administrative task for us. This has been a particularly busy year. The activities of the self-styled notification agencies referred to elsewhere in this report have created considerable extra work. We have received a large number of calls, e-mails and letters from those confused by the “official looking” notices they have received, or angry that they have been taken in and paid far more than the £35 statutory fee. There have been thousands of complaints about these businesses, including many from those who have responded and paid a substantial fee, sometimes when notification was not even required.

We have sought to address the activities of these businesses by working closely with the Office of Fair Trading, Trading Standards and local police forces to ensure that appropriate action is taken. The Office of Fair Trading has obtained injunctions against three such agencies and undertakings from several more. Convictions under Section 14 of the Trade Description Act 1968 have been obtained by Brent and Harrow trading standards service against one particularly active company and its director.

This has been the last full year in which we have dealt with the consequences of the move from the standard 3 year period of registration under the 1984 Act to the 1 year period of notification under the 1998 Act. Some 55,000 of the 1984 Act entries expired. During the year nearly 110,500 new notification applications were received and the register grew from 198,519 to 211,251.

We anticipate a very significant reduction in the number of fresh applications for notification, and expect that the major focus will be on renewals. We are also writing to all those who notified via an agency to alert them to the fact that they can renew direct with us and to instruct us to send all communications regarding their entry direct to them in future rather than the agency who submitted their original application. We hope to upgrade the platform on which our current notification system is based. We also intend to undertake a detailed study in preparation for commissioning a new computer system to handle the notification process. Among the priorities is to facilitate public access to the up-to-date register.

Information Line

The Information Line team continues to handle a very wide range of queries from callers as well as handling written enquiries. There continues to be a fairly high staff turnover and, as a consequence, a heavy recruitment and training requirement. A significant proportion of those who leave the team do

Case Study

BREACH: Security

Criminal Records Bureau (CRB)

The Criminal Records Bureau (CRB) produces Disclosure Certificates for Registered Bodies in England and Wales seeking criminal records checks on individuals in connection with their prospective employment.

A member of staff at one Registered Body who was Counter Signing Officer for such checks received a number of disclosure certificates at his home address rather than at his place of work. Copies revealing the officer's home address were also sent to potential recruits. The officer raised this matter several times with CRB without the matter being resolved. He then complained to the Commissioner.

Following contact with the CRB they undertook to revise their procedures to prevent similar disclosures happening again.

so to take up compliance posts elsewhere in the office for which they are well-equipped as a consequence of the thorough grounding they have in the practical application of the legislation. During the year the team handled some 4,500 calls a month, the great majority of which they were able to handle without the need to pass callers on to staff in our specialist sector teams.

We have been aware for some time that our telephone system has struggled to cope with the increased number of calls we have been receiving as the Office has expanded. We have recently upgraded our telephone equipment and intend to implement the new system by mid-2003. This will give us a real time picture of the number of calls we are receiving. It will also enable us to set up a number of overspill lines to cope with unforeseen peaks. When we have implemented this upgrade we will have a much better picture of the number of calls we are receiving. We will then review the staffing of the team with a view to increasing its complement as appropriate.

2) We will aim to ensure that policy makers give appropriate weight to individuals' rights.

Policy developments in the UK

One of the most significant areas for future public policy involved the government's consultation on proposals for 'entitlement cards'. The consultation document was substantial and set out a number of possible schemes. It was pleasing to note that the government fully recognised that this important issue raised substantial data protection and privacy concerns that must be addressed if any scheme is to proceed. To assist with the formulation of our response we commissioned research from a leading academic examining the wider social policy issues surrounding the introduction of such a scheme. To explore the issues in detail we held a conference with an impressive array of speakers, including the Home Secretary. We provided a very detailed response to the government's consultation, including the research commissioned as part of our own deliberations. In short, our view is that although there may be some benefits to individuals in having a secure and effective way to prove their identity, to establish a data protection compliant scheme would be a significant challenge and not one that is met by the current proposals. A framework of legal safeguards to guard against function creep, to prevent misuse and to ensure independent supervision would be necessary even if difficulties over the quality of the data and the practicalities of operating such an extensive scheme could be overcome.

Subject access

The Lord Chancellor's Department has been conducting its own review of subject access arrangements. This review, to which we responded, is both welcome and timely as the interface between these and the access rights under freedom of information legislation is of particular importance.

Retention of and access to communications data

The Anti-terrorism Crime and Security Act 2001 included provisions for communications service providers to retain communications data for national security related purposes. The data would be retained for longer than is necessary for the service providers' own business purposes. During the passage of the Act we expressed concerns as to whether such routine retention would be a proportionate response to the perceived problem - we still have these concerns. Nevertheless we have assisted the Home Office in developing a code of practice under which service providers could retain communications data for a limited period without breaching the Data Protection Act. A public consultation on this voluntary code has recently closed.

During the course of our discussions with the Home Office on the voluntary code we sought counsel's opinion on whether the routine retention of communications data might conflict with obligations under the Human Rights Act 1998. Although counsel thought this was unlikely he advised that access to the retained data did raise concerns. Where Parliament has decided that data can be retained expressly for purposes related to national security, there is a risk that those who use the Regulation of Investigatory Powers Act 1998 to access the data for a less pressing purpose will breach human rights. This is a point we have made in our response to the Government's consultation on access to communications data.

Other governmental consultations

In our response to a consultation following a review of the Rehabilitation of Offenders Act, we welcomed the suggestion for a Code of Practice on employers' use of information about individuals' criminal convictions and for a shortening of rehabilitation periods. We have continued to be represented on the Home Secretary's Task Force on Child Protection on the Internet and the Internet Crime Forum. Discussion on the mechanism for retention of fingerprint and DNA profile information following removal of the statutory requirement for deletion has continued. We have raised concerns about the Government's intention to go further, by means of an amendment to the Criminal Justice Bill, in enabling the police to take DNA samples and fingerprints from all those arrested and retain these whatever the outcome of the case.

In our response to a Treasury consultation on Proposed Amendments to the Money Laundering Regulations 2001, we commented on the proposal that additional personal data should be included with all wire transfers of money in order to implement a Financial Action Task Force special recommendation concerning terrorist financing. We expressed the view that an order should be made under Schedule 4, paragraph 4(2) of the Data Protection Act 1998 to place beyond doubt that transfers outside the European Economic Area of these additional personal data were necessary 'for reasons of substantial public interest'. We repeated this view in our response to the Treasury consultation on the Proposed Revision to the Money Laundering Regulations 1993 and 2001.

We have raised with the Financial Services Authority the data protection implications of financial institutions being required to undertake identity checks on existing customers.

Employment Practices Data Protection Code

We have continued work on our Employment Practices Data Protection Code. We are producing the code of practice to clarify what data protection law requires and to help employers negotiate this difficult area of the law. The sections on recruitment and selection, employment records and monitoring at work are available on our web site. We are now looking at the fourth, final section on medical records. The third section, dealing with monitoring at work, has attracted the most interest. The Code is designed to help employers determine whether any adverse impact on workers resulting from monitoring is justified by the benefits to the employer and others. Clearly, this can be a difficult balance to strike. The core principles of monitoring found in the Code are as follows;



- It will usually be intrusive to monitor your workers.
- Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment.
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered.
- Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified.
- In any event, workers' awareness will influence their expectations.

The section on monitoring was subject to a second, open consultation. As a result of this and other representations we received we have worked on its presentation to make it more useful to the various types of employers who carry out monitoring. We were sympathetic to those who criticised previous versions of the code for being too long, detailed and complex for small business, in particular, to use. Therefore we have removed much of the detailed, technical explanatory material to a separate ‘Supplementary Guidance’ document. This does not form part of the Code itself, but can be read alongside the Code by those wanting a more detailed explanation of the many issues covered in the Code itself. We have also produced a document entitled ‘Guidance for Small Businesses’. We have targeted this at the many small businesses that probably don’t have in-house lawyers or data protection specialists, yet who may well from time to time carry out monitoring of their workers, and who need to do so within the law. We are confident that the six page long summary of the main Code that we have produced for small business strikes the right balance between brevity and adequate explanation of a complex area.

We have certainly learnt a great deal from producing this Code of Practice. We are confident that our experience will help us in the future to produce the clear, practical guidance that will be most useful to employers and others in negotiating their potentially complex data protection compliance problems.

Criminal Justice

Following more than one hundred requests for assessment, we took enforcement action against the Prison Service as a result of their failure to provide timely responses to subject access requests. The Prison Service recognised the deficiencies in its procedures and has put in place measures to ensure future compliance.

The Association of Chief Police Officers in England, Wales and Northern Ireland and their Scottish counterparts have both revised their Codes of Practice for Data Protection to take account of the 1998 Act. The Codes were submitted to us for consideration under Section 51(4)(b) of the Act. Following wide consultation with data subjects and their representatives, and some further work on the Codes, we were pleased to confirm that they both promote the following of good practice in the processing of personal data.

We have helped the police develop guidance on the use of automatic number plate recognition technology. Information sharing initiatives are commonplace in the sector. We regularly give advice or make presentations on the impact of the Data Protection Act 1998 on crime and disorder partnerships. We have given advice to projects concerned with joining up a variety of criminal

Case Study

BREACH: Inaccurate personal data

Criminal Records Bureau (CRB)

An individual complained that a Disclosure Certificate provided to a prospective employer by CRB did not relate to her. Her surname was the same as the person whose police record was shown on the Certificate but all the other details (e.g. Christian name, date of birth etc) were different.

Contact with CRB showed that they had identified the mismatch of data and were taking action to correct this. They also undertook to retrain their staff to prevent similar errors in future.

justice information systems in each of Scotland, Northern Ireland and England and Wales.

On the freedom of information side we have encouraged and supported the development of model publication schemes for both police forces and police authorities. These are now being widely adopted.

We see data protection and, in time, freedom of information auditing as an important tool to help those both in the public sector and the private sector who handle information to meet their obligations. It is encouraging that increasingly businesses share this view and in many cases are using or adopting the audit materials we have made available to them. Although we can only audit data controllers ourselves where we have their consent, we are starting to do so. This is work we intend to take forward both with a view to developing and improving our audit materials as well as with a view to identifying common areas of non-compliance.

International developments

Influencing policy makers is not something that can be left to national data protection authorities alone. Electronic commerce spans the globe and governments work in concert with each other to deal with perceived problems. The regular meetings of European Data Protection Commissioners and the Annual International Conference of Data Protection and Privacy Commissioners provide valuable opportunities for issues of common interest to be addressed and common solutions found. It was our privilege to jointly host the 24th International Conference of Privacy and Data Protection Commissioners in Cardiff last September. The event was jointly hosted with our colleagues from the Republic of Ireland, Guernsey, Jersey and the Isle of Man. The central theme was 'Information Rights in the 21st Century - Confronting the Myths'. The conference provided for substantial debate amongst the 350 delegates and 40 data protection authorities from around the world. A key theme in the closed session for national data protection authorities was the response by their governments to the increased terrorist threat. The Commissioners concluded that unless an approach is taken by governments which give proper weight to data protection and privacy concerns there is a real danger that they will start to undermine the fundamental freedoms they are seeking to protect. Similarly an allied meeting of European Data Protection Commissioners issued a statement expressing collective concern at the mandatory systematic retention of telecommunications traffic data for use for law enforcement purposes that is now taking place in many countries.

The European Commission has undertaken its review of the implementation of the EU Data Protection Directive (95/46/EC) in member states. The Data Protection Act 1998 implements the Directive in the United Kingdom. The Commission embarked upon a substantial programme of research and consultation across the European Union. We played our part in ensuring that our own experiences were taken into account by providing a formal response to their consultation document and providing speakers at a special conference organised by the Commission. The Commission's First Report on the Implementation of the Data Protection Directive has recently been published. It concludes that the results of the review on balance militate against proposing modifications to the Directive at this stage.

The Working Party of European Data Protection Commissioners established under Article 29 of the Data Protection Directive continues to deal with many matters of common interest to the member states. In the past year it has issued some 15 working documents and opinions on a variety of issues ranging from on-line authentication services, the most widely reported of these being Microsoft 'Passport', through to electronic surveillance in the workplace. The Working Party is committed to further improving the transparency of its activities. We are eager to play our part in helping to achieve this by highlighting its activities within the UK.

During the year we have continued to take part in the work of both the Europol Joint Supervisory Body and the Customs Information System Joint Supervisory Authority. We continue to attend the Schengen Joint Supervisory Authority as an observer as part of our preparation for the UK's participation in the Information System from March 2004. The Information Commissioner has been appointed to the Joint Supervisory Body of Eurojust, the new European wide system of judicial co-operation. We have been represented at the first meetings of the Joint Supervisory Authority for Eurodac, the body involved with the comparison of fingerprints of applicants for asylum. In November 2002 we gave evidence to a sub committee of the House of Lords Select Committee on the European Union which was examining proposed changes to the Europol Convention.

This year we have continued to work with the Organisation for Economic Co-operation and Development (OECD). One of the Deputy Commissioners has worked with the secretariat and attended meetings of the Working Party on Information Security and Privacy which developed the revised Security Guidelines adopted in July 2002 and launched last autumn. Those Guidelines are an effort to develop a general awareness of information security issues, to encourage all those involved with systems to accept a degree of responsibility appropriate to their role, and to promote a general

Case Study

BREACH: **Retention of personal data**

A Police Force

A data subject complained that a Police Force had disclosed personal data about him to his employer that had resulted in him losing his job. At the time of the complaint a Police Force had held the information for over 3 years.

The information consisted of allegations about the data subject but no police action had been taken on these, the data subject had never been interviewed or charged and the force held no other information about him. Until the information was disclosed to his employer the data subject was unaware that the police held any data about him.

The Police Force were requested to delete the information as it had been kept for longer than was necessary for the purpose. They refused to do so and maintained that as the information had been regularly reviewed they could continue to retain it.

The Commissioner then informed the Police Force that he would be taking enforcement action against them. The Police Force then decided that in view of the time that had elapsed and as no further information about the data subject had come to their notice they would delete the data from their records.

'culture of security'. In the privacy field, OECD completed its work following the 1998 Ottawa Ministerial Declaration charging OECD with the task of producing practical guidance for the application of the 1980 Privacy Guidelines to global networks. The results of that work and the resulting practical policy guidance to member countries, businesses and individuals can be found in 'Privacy Online: Policy and Practical Guidance' published by OECD in 2002. The Working Party is now turning its attention to issues such as the impact of biometric identification technologies on privacy and the economics of trust. It will also wish to consider what messages on the importance of privacy and security for the online world can be brought to the attention of the World Summit on the Information Society to take place in Geneva at the end of this year.

Data protection continues to develop at an international level and we have continued to host visitors from around the world eager to learn from our experience. We continue to try to provide help and assistance to those newly established data protection authorities and have become involved in the European Union twinning programme. This involves providing technical assistance to the EU accession candidates. We have provided short term expertise on data protection and policing to the Czech Republic and are participating in a twinning project helping the Data Protection Commissioner for Cyprus. We also hope to build on previous work with the Maltese Data Protection Commissioner by participating in a twinning project to help establish the Commissioner's functions and train public sector workers in data protection awareness. We also took part in a peer review of the activities of the Hungarian Data Protection authority as part of an EU programme to assist accession countries on the path to full EU membership.

3) We will aim to ensure that those who handle information both in the public sector and the private sector are aware of their obligations and act accordingly.

During the year under review the Information Commissioner's Investigations Department has been particularly active in carrying out the field investigation of alleged criminal breaches of the Data Protection Act. This has involved:

- interviewing witnesses and obtaining witness statements
- obtaining and executing search warrants
- conducting tape-recorded interviews with suspected offenders, under caution

- reviewing evidence and preparing prosecution files; and
- forwarding files to the Legal Department with recommendations of prosecution, caution or no further action.

The offences under the Data Protection Act that represent the most significant mischief in terms of infringement of privacy are those under sections 55(1) 'unlawful obtaining' and 55(4) 'unlawful selling' of personal information. Some, but not all, private investigators and tracing agencies systematically and unlawfully obtain information from public and private sector organisations, usually by deception, and then sell that information on to their clients. The unlawful obtaining offence invariably has two victims - the 'data controller' from whom the information is obtained and the 'data subject' the person the information is about. The investigation of these offences is the main thrust of the department.

Baird Project

The Baird Project was a joint initiative between the Information Commissioner, the Department for Work and Pensions and the Inland Revenue. The purpose was to identify those persons and/or organisations that



unlawfully and systematically obtain, or seek to obtain, personal details from those agencies and then sell that information to their clients. The Baird Project concluded in March 2002. As a direct result of the project a number of cases have been brought to court during the year and there have been successful prosecutions. The success of the initiative has demonstrated that organisations can work

together for the benefit of all. Although the attachment of investigators from the Department for Work and Pensions and the Inland Revenue to the Information Commissioner's Investigation Department has concluded, the close links established by the Baird Project continue.

Regulation of Investigatory Powers Act 2000 - access to communications data

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a single regulatory regime for public authorities to access communications data. The regime is intended to be compliant with human rights legislation, through RIPA's explicit statutory requirement to take account of necessity and proportionality when accessing communications data. RIPA also provides for statutory oversight of the exercise of powers and duties under the legislation, and for a statutory mechanism to complain about the exercise of those powers and duties. Within RIPA there is a list of authorities that Parliament has

Case Study

BREACH: **Principle 6 – failure to** **comply with an** **individual's Subject** **Access Rights**

HM Prison Service (HMP)

An individual complained that HMP had delayed their response to his subject access request for data for use in relation to the review of his "Category A" Prisoner status. His case proved to be one of a substantial number of subject access cases to HMP that had been subject to lengthy delays.

HMP acknowledged that it was having problems dealing with subject access requests within the 40 day time limit and that a sizeable backlog of cases had built up.

Subsequently the Commissioner served an enforcement notice on HMP requiring them to clear the backlog of cases by 30/4/03 and to take steps to ensure that subject access requests were dealt with promptly in future.

agreed should enjoy lawful access to communications data. They are primarily law enforcement and intelligence agencies, namely police forces, the National Criminal and Intelligence Service, the National Crime Squad, HM Customs & Excise, the Inland Revenue, the Security Service, the Secret Intelligence Service and the Government Communications Headquarters. Parliament may put additional public authorities on the list. The Information Commissioner is one of the additional public authorities proposed to be named in an Order to allow access to communications data under RIPA. We require communications data for evidential purposes when investigating and prosecuting offences under the Data Protection Act 1998. A public consultation document entitled, "Access to Communications Data – Respecting Privacy and Protecting the Public from Crime" was released in March 2003. We have responded to this consultation document.



Credit referencing

My predecessors have commented in previous reports on the use of third party data in the consumer lending process. 'Third party data' in this context is personal information about another individual, typically husband or wife or partner. Following Tribunal Decisions, and Enforcement Notices agreed between the credit reference agencies and the (then) Data Protection Registrar in April 1992, third party data includes information on individuals other than the credit applicant, where the third party has resided concurrently with the credit applicant and it is reasonably believed that the third party has been living as a member of the same family as the applicant in a single household. In late 2000 in response to continuing concerns the consumer credit industry proposed new procedures for processing third party data. We recognised these procedures required major changes to existing systems and that these would take time to implement. Two years into the change-over period it is time for the industry to set a realistic but firm date by which the new procedures will be in place and fully operational. We have now asked those represented on the working party which drew up the new procedures to propose a firm date. We believe that the date set should be before the end of 2004 at the latest.

Unsolicited marketing

We have continued to deal with a large number of complaints about unsolicited marketing, particularly by fax. As detailed elsewhere in the report, we have taken formal action against a number of fax marketers. Encouragingly, however, in the last few months there has been a marked decrease in the number of complaints in this area. We hope it is not too optimistic to suggest that this indicates that most of those who market by fax are now fully aware of their obligations under the Telecommunications (Data Protection and Privacy) Regulations 1999.

Small businesses

In July 2002, recognising that small businesses may be confused by their data protection obligations, we produced "The Data Protection Act and You." This was a short and straightforward leaflet aimed specifically at the needs of small businesses. It explains how to stay within data protection law and emphasises that data protection compliance is 'good for business'. We are looking for further ways to present data protection compliance advice to small businesses simply but effectively.

Enforcement strategy

In August 2002 we published our enforcement strategy following the review conducted during the previous year. The Enforcement Board has met on a number of occasions since then. The Enforcement Team was recruited from our Compliance, Investigations and Legal departments and began its work in February 2003. The Team was set up to proactively investigate and enforce where necessary in areas of non-compliance identified by the Board.

Last year saw the completion of a study commissioned from the University of Manchester Institute of Science and Technology into data protection compliance by UK websites. The mixed findings of this report encouraged our Enforcement Team to carry out its first investigation into website compliance. In April 2003 the team carried out a survey of 99 travel-related websites, focussing on their compliance with the 1st data protection principle when obtaining personal data on-line. The survey looked at small, medium and large scale companies.

The survey showed that there appeared to be no deep founded or widespread problem of non-compliance with the Act amongst the websites studied. Although there was variation in the quality of the fair processing information provided to individuals, the vast majority were found to provide some form of fair processing information or appeared to process personal data obtained for purposes wholly within the reasonable expectations of the data subject.

A small number of websites were found not to provide any form of fair processing information, which is a matter of some concern. We wrote to the respective data controllers for these websites and appropriate advice and guidance was given. Monitoring of these sites is ongoing to establish whether or not the advice results in them making the necessary alterations.

The Enforcement Board also considered issues surrounding the exercise of the right of subject access in the context of manual records held by central government departments. Our own compliance team visited a number of departments to inspect their paper files. Following these visits it was decided

to assist data controllers with compliance by developing checklists to enable them to identify which files are likely to fall within the scope of the Data Protection Act. Because of the interface between data protection and freedom of information compliance it was also agreed to produce practical guidance about access to information under both pieces of legislation.

Enforcement Work

21st Century Faxes Ltd, Info 4 U Ltd, Right 2 Vote Ltd, Hyperos Systems Ltd, Green Freephone Pages Ltd, Launchasset Ltd, the Lord's Witnesses; Voucher Heaven Ltd and two directors.

Formal enforcement action was taken against seven of the above companies and two directors in relation to contraventions of the Telecommunications (Data Protection and Privacy) Regulations 1999 in respect of sending of unsolicited direct marketing faxes. The Enforcement Notice served upon the companies and directors concerned their compliance with Regulations 23 and 24 of the Telecommunications Regulations. The companies and the directors concerned appealed against the Enforcement Notice.

Regulation 23 prohibits the sending of unsolicited direct marketing material by fax to individual or corporate subscribers who have objected either specifically to the sender in question (Regulations 23 (2)(a)) or generally by registering with the Fax Preference Service (FPS) (Regulation 23 (2)(b)). Regulation 24 prohibits the sending of direct marketing material by fax to individual subscribers without their prior consent.

The enforcement action was based on numerous complaints received by the Commissioner. The original Enforcement Notice was withdrawn against Launchasset Ltd and one of the directors. A revised Enforcement Notice was served on the six remaining companies, the remaining director and one additional company, Voucher Heaven Ltd.

Whilst preparations for a substantive appeal hearing before the Tribunal continued, further discussions and negotiations took place between the Commissioner and the companies involved. These discussions proved fruitful. The companies agreed to withdraw their appeal and not to appeal against a revised notice, and the individual agreed to provide an undertaking that any company of which he is, or becomes, a director, will comply with the notice.

Petworth Publishing Ltd and a Director

This is another case where formal enforcement action was taken in relation to contraventions of the Telecommunications (Data Protection and Privacy) Regulations 1999 in respect of unsolicited direct marketing faxes. The

enforcement action was based on numerous complaints received by the Commissioner. Neither the business nor the individual appealed against the Enforcement Notice.

4) We will aim to ensure that individuals are aware of their rights to information, and feel confident that those rights are respected and can be exercised.

Freedom of Information

a) Approval of Publication Schemes

Section 19 of the Freedom of Information Act places an obligation on public authorities to adopt publication schemes and, having obtained approval for those schemes from the Commissioner, to publish information according to those schemes. The Act envisages two types of scheme. "Bespoke schemes" are those designed for particular authorities, for instance a central government department. They will be individually approved. Model schemes, by contrast, are designed for cases where a large number of public authorities may wish to adopt the same scheme, for instance parish councils or police forces. Individual approval is only required if an authority wishes to depart from the model.

The following table sets out the timetable for approval of schemes by the different classes of authorities:

Sector	Submissions accepted from	Final deadline	Scheme active
Central Government, some NDPBs	1st July 2002	30th September 2002	30th November 2002
Local Government	1st October 2002	31st December 2002	28th February 2003
Police and Prosecuting bodies	1st February 2003	30th April 2003	30th June 2003
Health Service	1st June 2003	31st August 2003	31st October 2003
Education, remaining NDPBs and publicly owned companies	1st October 2003	31st December 2003	29th February 2004
Other public authorities	1st February 2004	30th April 2004	30th June 2004



A key component of our work during the past 12 months has been the development and approval of model schemes. The following have been approved:

Port Health Authorities
Parish Councils
Parish Meetings
Police Authorities
Police Forces
Magistrates Court Committees
Fire Authorities
Internal Drainage Boards
District Drainage Commissioners
Passenger Transport Authorities.

Model schemes for the Health sector wave in England have also been approved for the following:

Acute Trusts
Strategic Health Authorities
Primary Care Trusts
Opticians and Optometrists
Mental Health Trusts
General Practitioners
Dentists
Community Pharmacists
Ambulance Trusts

Equivalent models for Wales and Northern Ireland are expected to be approved shortly.

Adoption rates within the first wave of schemes has been good, with 257 schemes approved. Only one public authority in this wave is known to have not yet submitted a satisfactory scheme for approval. Within the second wave, some 456 primary local authorities (districts, counties and unitaries) have submitted and had schemes approved. Some 7,000 model schemes have been adopted, principally by parish councils and parish meetings. Our estimate is that some 5,000 of these bodies have failed to adopt schemes, although in the absence of a comprehensive list, it is impossible to be precise. In addition to parish councils and meetings, port health authorities have been slow to meet their obligations under the Act.

It is important to recognise the work put into developing such schemes by all of the representative bodies concerned including the National Association of Local Councils, the Association of Chief Police Officers, the Association of Port Health Authorities, the Association of Police Authorities and the NHS Project Board. We also take this opportunity to thank the Lord Chancellor's Department for its work in ensuring that central government departments and NDPBs have been aware of their obligations and of the deadlines for adoption imposed by the Act .

b) Comments on publication schemes adoption and approval

To date, there have been very few complaints received from the general public about failures to publish information according to schemes, although it should perhaps be noted that there has been little publicity given to their existence.

As noted, schemes must be approved by the Commissioner. Our initial approval criteria were set at a low level as experience was lacking both in this Office and in public authorities in general as to the sort of information which should or could be included within a scheme. Generally speaking the schemes submitted to us have described information already being published by public authorities, and have only included small amounts of new information. We have made it clear, however, that in keeping with the spirit of the way in which publication schemes were described in the course of the passage of the Freedom of Information Bill that those criteria will be revised before existing schemes are due for renewal. The Commissioner's expectation is that future schemes will set out the intention to publish routinely information which was previously not available at all or only made available on request.

A recurring problem in bespoke schemes has been confusion between individual rights of access and routine publication in accordance with a publication scheme. Initially there were problems in two areas.

Many schemes initially required requests for publication scheme material in writing, as is indeed required in the case of requests submitted under section 1 of the Act. It has been necessary to make clear to public authorities that once a scheme has been approved, information must be made routinely available through it and that while, as when someone orders books, there may be a slight delay before information is provided, there should be no question of information described in a scheme having to be located and edited in response to individual requests.

A number of the bespoke schemes submitted specified fees for the location and supply of documents. It has been pointed out to these authorities that publication scheme material should be routinely and readily available and

Case Study

BREACH: Principle 6 – failure to comply with an individual's subject access rights

An individual complained that soon after starting a new job he was dismissed by his employer due to a personal reference his employer believed was unsatisfactory. The complainant requested a copy of the reference under Section 7 of the Act, in order to assess the accuracy of its contents. Further to this, the complainant was concerned that unless he was able to view the contents of the reference he would have difficulty finding new employment as he would be unsure of supplying future references. The complainant's employer refused to release the document in question on grounds of confidentiality.

The Information Commissioner's Office contacted the employer and detailed a list of points a data controller must consider when he receives a subject access request for information which includes disclosures about third parties. After considering this advice the employer agreed to release an edited version of the references to the complainant, with the identities of third parties blanked out.

therefore not be subject to location and retrieval charges. (Authorities may, of course, continue to charge in the normal way for certain publications if that is their current practice.)

In model schemes the representative bodies have generally worked closely with our FOI team and hence have not experienced the same problems in the development of the schemes.

Some bespoke schemes, particularly those developed by public authorities other than central government departments, have provided encouraging signs that some authorities are beginning to take to heart the message that they should consider publishing information which is not currently made available.

The purpose of publication schemes is to promote greater openness. It is important not to allow the business of the development of models, the submission of schemes and the application of approval criteria to obscure this central goal. As part of the ongoing review of the operation of publication schemes and the approvals process which will be initiated during the course of 2003-4, we will consider ways of reducing the administrative burden on public authorities while achieving the purpose of the schemes.

c) Raising awareness and building strategic alliances

Raising awareness of the Act has also been a major part of our work over the past year. We have had the opportunity to address a variety of audiences across the public sector, whether through short presentations and informal meetings or large formal conferences. We are particularly grateful to the Joint Information System Committee and NHS Project Boards for the opportunities which they have made available to us.

We hope that over the coming year the relationships which we have developed in the higher education and health sectors, together with those with the Lord Chancellor's Department, the Parliamentary Ombudsman, the National Archives and bodies such as the Campaign for Freedom of Information can be built upon. These relationships will become increasingly important as we develop our thinking around the exemptions and other elements of the Act which will come into play once rights under section 1 of the Act come into being in January 2005.

With the Parliamentary Secretary for the Lord Chancellor's Department, the Commissioner jointly chairs the Lord Chancellor's Advisory Group on the Implementation of the Freedom of Information Act. The Group provides an effective focus for the activities, concerns and ideas of the interested parties represented. We have welcomed the opportunity to take part in the events

organised under the auspices of the Group aimed at developing awareness across the public sector.

d) Preparing for 2005

During the latter part of the year, the Commissioner took the opportunity to review his own preparations for the full implementation of the Act in 2005. The key decision was to defer the proposed integration of FOI and data protection compliance work until at least the middle of 2005, thus allowing for the focussing of a dedicated resource upon the task of preparation and policy development. One of the existing Assistant Commissioners was tasked with organising a new FOI department within the Office and developing a project plan for implementation.

Electoral registration

In the past we have expressed concern about the widespread availability of the electoral register and its use for many different purposes. The Representation of the Peoples Act 2000 established a framework where there would be two versions of the electoral register. There would be a full version available for use only for electoral and other limited purposes and another edited version that could be made available for sale for any purpose. Individuals should now be given the choice to 'opt out' of the edited version should they so wish. After some delay the necessary Regulations are now in place, meaning that for the first time individuals are being given a choice over the use and disclosure of the information they provide for electoral purposes. Whilst we have some concerns over the prominence and wording of this choice on some canvass forms, the provision of a choice is a welcome step forward. We look forward to seeing how well these arrangements work in practice, and in particular how well individuals understand and exercise the choice they now have.

The right to know campaign

Our advertising campaign in 2002 had the purpose of increasing the public's awareness of their rights under the Data Protection Act and in particular the right to access information about them.

With a complex message and a target audience of the whole population, the most cost effective media option available was specialist press and national press supplements. Magazines such as 'Cosmopolitan', 'Reader's Digest', 'GQ' and 'Now' were used in conjunction with 'Independent', 'Sunday Times' and 'Guardian' supplements.



Information Commissioner – Annual Report and Accounts 2003

We ran three adverts which asked direct questions to the audience and used emotive words to provoke public reaction and interest in information issues.

Working with the media

Once again we have continued to invest in supporting media journalists and editors in covering data protection and freedom of information issues over the year.

In October 2002 we appointed Citigate Communications to undertake some of our PR functions for a six month term. In April 2003 this contract was extended for a further twelve month period. This involves them operating a full Press Office function for us.

Chapter 2:

Some challenges we face



A surveillance society?

At the 24th International Data Protection Commissioners' Conference in Cardiff, the assembled Commissioners spoke with one voice in expressing concern that in the fight against terrorism and serious criminality, governments providing for greater intrusion into individuals' private lives run the risk that this will undermine the fundamental freedoms that they are trying to protect. A significant challenge for us in the data protection community is to ensure that policy makers weigh privacy and data protection concerns before embarking on potentially intrusive initiatives.

At the international level we are already working closely with our colleagues on the Article 29 Working Party in response to the requirements of foreign governments, particularly the United States, to have access to airline passenger reservation details. It will be vitally important that understandings are reached at international level that strike the right balance between safeguarding data protection rights and protecting against any terrorist threat.

At home the Government is consulting on a voluntary code of practice for the prolonged retention of communications data on their customers by communication service providers. The data are to be available to law enforcement bodies for national security purposes. Similarly, the Government is consulting on who should have access to communications data for more general law enforcement purposes. Within this latter consultation there is a welcome call by the Home Secretary for a wider public debate on the balance to be struck between privacy and protecting the public from crime. It is our intention to help foster, and to contribute to this debate. It is a concern that the way we live our lives today, with increasing use of technologies that record our activities as never before, we run the risk that, piece by piece, we are seeing the creation of an infrastructure for a surveillance society. It is important that we take a step back and examine the wider picture and that



Case Study

CONVICTED: Unlawfully obtaining and disclosing

Alistair Fraser, trading as Solent Credit Control in Portsmouth, pleaded guilty at East Hampshire Magistrates Court on 21 August 2002 to offences of unlawfully obtaining and selling personal information in breach of the Data Protection Act 1998. He asked for 66 similar offences to be taken into consideration.

The prosecution was brought by the Information Commissioner as a result of the BAIRD project.

In this instance, the personal information had been unlawfully obtained by Fraser from the Department for Work and Pensions by means of, what is sometimes known as 'blagging', or making 'pretext enquiries'.

The Magistrates fined Fraser £1,400 in total and ordered him to pay £1,000 costs.

our approach to personal privacy and data protection ensures that we do not, albeit unwittingly, create a society in which none of us would chose to live. We are well placed to try to assess the bigger picture as these developments come forward, be these proposals for entitlement cards or for wider access to communications data. The challenge in the year ahead is to ensure that we influence thinking and developments so that the personal privacy and data protection aspects are fully recognised and addressed. We aim to rise to this challenge and help stimulate a sensible discussion during the year ahead.

One area of surveillance where we have taken a lead in setting appropriate standards is with CCTV surveillance. We issued a data protection code of practice about this which is now 3 years old. The variety of video surveillance applications now deployed has increased. The recording of digital images, the use of automatic number plate recognition and automated facial recognition are now much more widespread in a large number of different contexts, ranging from congestion charging to retailing. We are therefore going to review our existing code in the light of our experience of its operation and any gaps created through technological change. This is a big task and we have many people to consult but it is intended that a revised code dealing with video surveillance will be published by the time of our next annual report.

Enforced subject access

We have, almost since UK data protection law first came into effect in the second half of the 1980s, drawn attention to the practice of enforced subject access to police records. Typically this takes place when, prior to confirmation of a job offer, an employer requires a prospective worker to use his or her right of subject access to obtain a copy of a police record. This then has to be presented to the employer who takes it into account in deciding whether to confirm the offer.

This is an abuse of the right of access which is a central plank of data protection law, given to data subjects for their benefit rather than for the benefit of third parties. In addition it undermines the important public policy objective of enabling those with criminal records to put their pasts behind them to which effect has been given in the Rehabilitation of Offenders Act 1974. This is because an individual's police record will contain details of all convictions whether or not they are spent. The importance of rehabilitation has been underlined by the recently completed review of the 1974 Act which recommended that, in general, rehabilitation periods should be shortened.

We therefore welcomed the measure introduced by the then Home Secretary, through section 56 of the Data Protection Act 1998, to make enforced subject access in many cases, a criminal offence. This was contingent on the

system of criminal conviction and criminal record certificates also known as "disclosures" introduced by the Police Act 1997 coming fully into operation. This provides a controlled mechanism for employers to gain limited access to workers' criminal records.

Whilst we are keen that section 56 should be brought into effect as soon as possible there appear to be two obstacles. Firstly there is the question of Northern Ireland. Although the Criminal Records Bureau (CRB) has been established for England and Wales and a similar arrangement is in place in Scotland, as far as we are aware there are no plans to introduce a comparable system in Northern Ireland. Secondly, it appears likely that as a result of an independent review of the Criminal Record Bureau's strategies and operations the launch of basic disclosures in England and Wales is to be postponed indefinitely. It therefore seems that the day on which the relevant sections of the Police Act 1997 are all in force across the whole of the UK might never arrive.

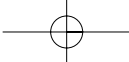
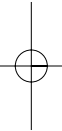
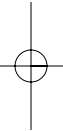
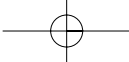
Without Government intervention there appears to be little prospect that the objective of outlawing enforced subject access will be achieved in the foreseeable future. However, the CRB is up and running, at least as far as standard and enhanced disclosures are concerned, so those cases where potential employers have the most pressing need for access to criminal conviction information are now covered. The challenge for us is to persuade the Government to bring section 56 of the Data Protection Act 1998 into force even though all the mechanisms envisaged in the relevant sections of the Police Act 1997 are not yet in place. This may well require primary legislation but without it the important principle of rehabilitation will continue to be subverted.

Telecommunications issues

In the course of enforcement action against fax marketers it has become apparent that sophisticated telephony packages can cause a fax to be sent to a number which is not registered on the Fax Preference Service stop-list by it being diverted to a fax machine linked to a number which is registered. Similar problems can arise where a non-geographic number, for example an 0800 number, has been registered by the subscriber but the underlying geographic number, which the subscriber may well be unaware of, has not. There is a broad education and awareness task here in which the industry, including equipment manufacturers and suppliers, network operators and service providers, as well as this Office and the Fax Preference Service have parts to play.

Information Commissioner – Annual Report and Accounts 2003

We are beginning to receive a number of complaints about unsolicited e-mails. Regulations to implement the Privacy in Electronic Communications Directive (2002/58/EC) are scheduled to be brought into force in October this year and will replace the Telecommunications (Data Protection and Privacy) Regulations 1999. The new Regulations will expressly apply to e-mail and provide that, unless an e-mail address has been obtained in the context of an existing relationship with the individual concerned, prior consent is required before unsolicited marketing communications can be sent. Formal regulation has an important part to play, not least by helping reinforce acceptable norms and thus strengthening the grounds on which ISPs can take action against those who send unsolicited commercial e-mails. However, particularly in the light of the fact that much of it initiates from outside the EU, giving rise to obvious investigative and jurisdictional difficulties, it is not a panacea. We intend to explore the possibility of identifying sources of authoritative and regularly updated advice for internet users on the practical steps they can take to minimise the chances of receiving unsolicited e-mails.

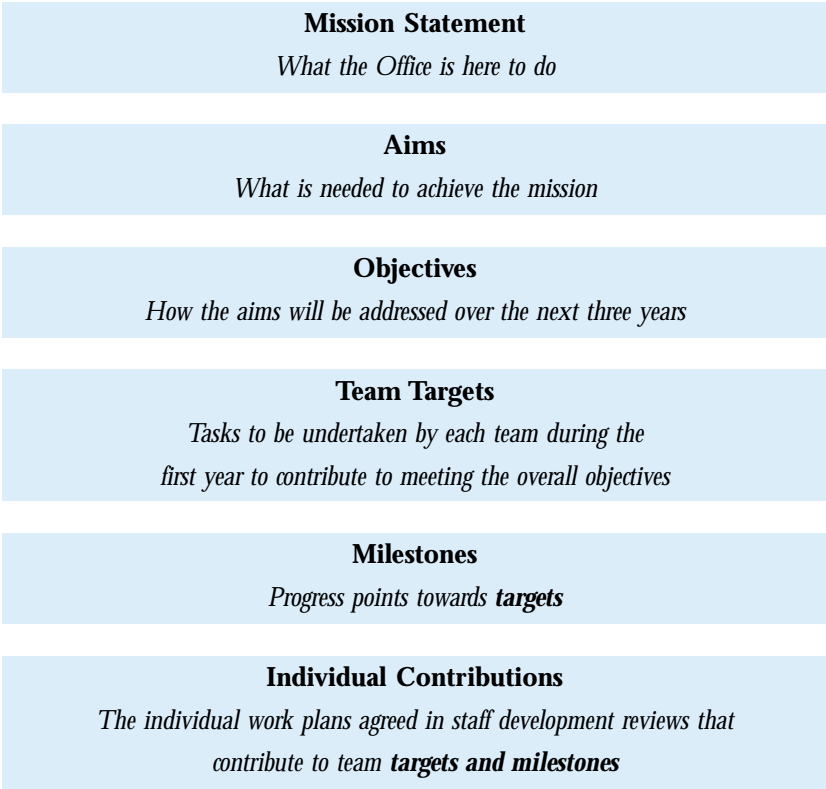


Chapter 3:

The year ahead



The overall Corporate Strategy is designed to ensure that activities cascade through the following stages:



The Commissioner's Mission, Aims and Objectives will be reviewed during the course of 2003 – 4. This review is likely to include a full analysis of the environment in which the Office is operating, possible re-casting of the Mission, Aims and Objectives and an up-dated statement of strategic direction and priorities.

Dominating all our plans, we will ensure that our priorities address the major challenges we face:

Challenges	Priorities
Implementation of Freedom of Information Act and other access laws.	Developing from a mature data protection organisation into the champion of both public openness and personal privacy.
Rising public concern over data protection issues.	Maximising our effectiveness and influence: <ul style="list-style-type: none">• more proactive• influential profile• strong at communicating• successful promotion of good practice• enforcement targeted on mischiefs causing real detriment.
Rapid changes – technology, law, policy, and public concerns.	
Modernising government agenda.	Enlarging/modernising our office: <ul style="list-style-type: none">• successful Change Programme• Multi-site operation• improved governance, structures and systems• improved knowledge management• useful service delivery targets and other ways to be sure we are succeeding• ensuring our staff achieve their full potential• accommodation needs.
Growth of international activity.	
How best can we make a difference?	Initiating and responding to major policy initiatives.
	Getting the best from our international work.

Case Study

CONVICTED:
Unlawfully obtaining

Despite the fact he made no known use of the information seen, an employee was convicted of unlawful obtaining of personal data when he accessed records on his employer's computer system for his own purposes and not in the course of his employment.

This Business Plan is available in full on our website and sets out the main activities which we will be carrying out during 2003-4. It shows what each Team will be doing (whether proactively or in response to external demands and events), and where responsibilities lie.

Case Study

CONVICTED: Unlawfully obtaining and disclosing

Karen Pritchard and Jacqueline North, trading as 'V Chasers' in Brecon, South Wales, and Karen Pritchard, trading as 'V Chasers 2000', pleaded guilty at Brecon Magistrates Court on 18 November 2002 to (36 and 2 respectively) offences of unlawfully obtaining and selling personal information in breach of the Data Protection Acts 1984 and 1998.

Pritchard asked for 348 and North for 60 similar offences to be taken into consideration.

This was another prosecution brought by the Information Commissioner as a result of the BAIRD Project.

In this instance, the personal information was unlawfully obtained by Pritchard and North from the Department for Work and Pensions (then the Benefits Agency) by means of deception.

The Magistrates fined Pritchard a total of £2000 with £600 costs and fined North £300 with £300 costs.

Our team plans cover both "casework" and key "projects, initiatives and events" for the year ahead. The nature of our organisation makes it impossible to adopt complete consistency across these plans, but such diversity is one of our strengths.

This is the first year the Business Plan has adopted this structure and approach. There will inevitably be a need to fine-tune the Plan, for this and future years, as it starts to be used as the principal instrument for guiding our work and shaping our future.

Amongst the projects, initiatives and events for the year the following milestones have been extracted.

- *To conduct a review of our Mission, Values, Aims and Objectives for inclusion in the 2004-2007 Corporate Plan.*

- *To adopt meaningful improvements to management information including adoption of service delivery standards by December 2003.*

- *To finalise and adopt an implementation plan for FOI work by August 2003.*

- *To put in place improved Corporate Governance arrangements for the organisation by November 2003.*

- *To establish offices within the devolved administrations by March 2004.*

- *To initiate a review of data protection regulation to identify changes of law (primary and secondary), policy or practice which would improve effectiveness or remove unnecessary burdens, by August 2003.*

- *To meet security standards laid down in ISO17799/BS7799 by January 2004.*

Information Commissioner's Accounts for the year ended 31st March 2003



Accounts Contents

	Page
Foreword	44
Statement of Responsibilities	49
Statement on Internal Control	50
Certificate and Report of the Comptroller and Auditor General	54
Income and Expenditure Account	56
Balance Sheet	57
Cashflow Statement	58
Notes to the Accounts	59

Foreword



Introduction

The annual accounts have been prepared in a form directed by the Lord Chancellor with the consent of the Treasury in accordance with paragraph (10)(1)(b) of Schedule 5 to the Data Protection Act 1998.

Under paragraph 10(2) of Schedule 5 to the Data Protection Act 1998 the Comptroller and Auditor General is appointed auditor to the Information Commissioner.

History

On 12 June 2003 responsibility for the Information Commissioner passed to the newly created Department for Constitutional Affairs. Previously responsibility for the Information Commission had passed to the Lord Chancellor's Department from the Home Office following the Governments Machinery of Government changes announced in June 2001.

Following implementation of the Data Protection Act 1998 on 1 March 2000, the corporation sole by the name of Data Protection Registrar, established by the Data Protection Act 1984, continued in existence but under the name of the Data Protection Commissioner.

The Freedom of Information Act 2000 received Royal Assent on 30 November 2000. The title of the Data Protection Commissioner changed to the Information Commissioner with effect from 30 January 2001.

Principal Activities

The Information Commissioner has responsibilities and duties under the Data Protection Act 1998 and Freedom of Information Act 2000.

The main purposes of the Data Protection Act 1998 are to:

- make the nature and use of personal data in computer systems and structured manual records open to public scrutiny (through promoting and enforcing the data protection principles);
- ensure good practice in the use, processing and protection of personal data in computer systems and structured manual records (through promoting and enforcing the data protection principles); and
- allow individuals to claim compensation for damage and any associated distress arising from any contravention of the requirements of the Data Protection Act.

During the year the Office has continued work to implement the Freedom of Information Act 2000.

The main purposes of the Freedom of Information Act 2000 are to:

- provide for the general right of access to recorded information held by public authorities and to specify the conditions which need to be fulfilled before an authority is obliged to comply with a request for information; and
- establish the arrangements for enforcement and appeal.

The Office is not a typical Non-Departmental Public Body. Such bodies usually have a relationship with Ministers which is based on the delegation of Ministerial powers. The Commissioner is an independent body created by statute who reports directly to Parliament. He is required to carry out those functions laid down in the Data Protection Act 1998 and Freedom of Information Act 2000, using only those powers which these Acts set out. All his decisions are subject to the supervision of the Information Tribunal and the Courts.

The Commissioner is responsible for setting the priorities for his Office, for deciding how they should be achieved, and is required annually to lay before each House of Parliament a general report on performance.

The Commissioner also has responsibilities in relation to the Consumer Credit Act 1974, the Telecommunications (Data Protection and Privacy) Regulations 1999 and in respect of European wide law enforcement systems. The Commissioner is the UK national supervisory authority for Europol, Eurodac, and the Customs Information System and is a member of the

Europol, Eurodac, Eurojust and CIS Joint Supervisory Authority. The Commissioner is also the designated national supervisory authority for the Schengen Information System (SIS) and attends the SIS Joint Supervisory Authority as an observer prior to the UK accession.

Fuller details of the Commissioner's activities, and progress towards his objectives during the year, are given elsewhere in the annual report.

Results for the Period

The results for the year and the Commissioner's financial position at the end of the period are shown in the attached accounts.

The retained surplus for the year transferred to reserves is £56,386.

The Information Commissioner has been financed by a grant-in-aid from the Lord Chancellor's Department.

Payments for the year have been apportioned between activities as below. As the Office expands in readiness for the full implementation of the Freedom of Information Act 2000, many costs can be attributed to both data protection and freedom of information functions, and thus reasoned estimates have been used to apportion costs.

	Grant in aid	Payments
	£	£
Data Protection	5,500,000	5,498,860
Freedom of Information	3,126,000	3,126,869
IT Modernisation	4,000,000	4,000,000
Grant-in-aid carried forward	<u>709</u>	<u>980</u>
	<u>12,626,709</u>	<u>12,626,709</u>

Fees

Paragraph 9(1), Schedule 5 of the Data Protection Act 1998 provides that all fees and other sums received by the Commissioner in the exercise of his functions under the Act or section 159 of the Consumer Credit Act 1974 shall be paid by the Commissioner to the Lord Chancellor. Fees and sundry receipts received prior to 31 March 2002 were remitted to the Secretary of State for the Home Department

Changes in Fixed Assets

This has been the second year of a two year programme to modernise the Office IT systems. A new IT infrastructure is now in place and an IT case-working system is in development. More details on fixed assets are given in note 8 to the accounts.

Future Developments

Full individual rights of access under the Freedom of Information Act 2000 come into force for all public authorities in January 2005. The Office will continue to approve publication schemes prepared by public authorities in the coming year in accordance with the timetable laid down by the Lord Chancellor and will continue to expand accordingly to meet projected workloads.

Post Balance Sheet Events

Lord Chancellor's Department

On 12 June 2003 the Government announced its intention to abolish the post of Lord Chancellor and for the work of the Lord Chancellor's Department to be taken over by a new Department for Constitutional Affairs. It is not anticipated that this constitutional change will materially affect the funding of the Information Commissioner's Office for the year ending 31 March 2004.

Charitable Donations

No charitable donations were made in the year ended 31 March 2003.
(2001/2002 - £nil)

Employee Policies

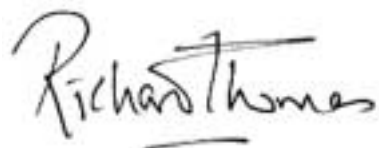
The Commissioner's Equal Opportunities policy aims to ensure that no potential or actual employee receives more or less favourable treatment on the grounds of race, colour, ethnic or national origin, marital status, sex, sexual orientation, disability or religious belief.

The Commissioner continues to place importance on ensuring priority is given to the provision of appropriate training so that staff can develop skills and understanding of their roles in line with the aims and objectives of the Office.

Maintenance of the provision of information to, and consultation with employees continues to be managed through a staff intranet and regular meetings with Trade Union representatives. A formal Health and Safety Policy and Manual is available to all members of staff. A Health and Safety Committee is in place to address health and safety issues.

Compliance with Public Sector Payment Policy

The Office has adopted a policy on prompt payment of invoices which complies with the 'Better Payment Procedure Code' as recommended by Government. In the year ending 31 March 2003, 96.3% (2001/2002 – 95.8%) of invoices were paid within 30 days of receipt or in the case of disputed invoices, within 30 days of the settlement of the dispute. The target percentage was 95%.



Richard Thomas
Information Commissioner
24 June 2003

Statement of the Information Commissioner's Responsibilities



Under paragraph 10(1)(b) of Schedule 5 to the Data Protection Act 1998 the Commissioner is required to prepare in respect of each financial year a statement of account in such form as the Lord Chancellor may direct. The accounts are prepared on an accruals basis and must give a true and fair view of the Information Commissioner's state of affairs at the year end and of his income and expenditure, total recognised gains and losses and cash flows for the financial year.

In preparing the accounts the Commissioner is required to:

- observe the Accounts Direction issued by the Lord Chancellor with the approval of the Treasury, including the relevant accounting and disclosure requirements, and apply suitable accounting policies on a consistent basis;
- make judgements and estimates on a reasonable basis;
- state whether applicable accounting standards have been followed, and disclose and explain any material departures in the financial statements;
- prepare the financial statements on the going concern basis, unless it is inappropriate to presume that the Information Commissioner will continue in operation.

As the senior full-time official, the Commissioner 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 and for the keeping of proper records, are set out in the Non-Departmental Public Bodies' Accounting Officer Memorandum, issued by the Treasury and published in Government Accounting.

Statement on Internal Control



As Information Commissioner and Accounting Officer, I have responsibility for maintaining a sound system of internal control that supports the achievement of my policies, aims and objectives, whilst safeguarding the public funds and assets for which I am personally responsible, in accordance with the responsibilities assigned to me in Government Accounting.

The system of internal control is designed to manage rather than eliminate the risk of failure to achieve policies, aims and objectives; it can therefore only provide reasonable and not absolute assurance of effectiveness.

The system of internal control is based on an ongoing process designed to identify the principal risks to the achievement of my policies, aims and objectives, to evaluate the nature and extent of those risks and to manage them efficiently, effectively and economically. This process has been in place for the year ended 31 March 2003 and up to the date of approval of the annual report and accounts and accords with Treasury guidance.

As Accounting Officer, I also have responsibility for reviewing the effectiveness of the system of internal control. I have established the following structures and/or processes:

- a Management Board, comprising both Deputy Commissioners, my Legal Adviser, my Director of Personnel and Finance and my Director of Marketing and Communications, which meets formally one week each month and informally most other weeks to consider the plans and strategic direction of the Office;
- a Senior Management Group in addition to the Management Board, which comprises the Management Board members together with the various departmental managers, which meets on a monthly basis, the

format of the meeting alternating between formal and informal meetings. These meetings provide monthly updates from managers which assist in the monitoring of identified risks;

- production of a Corporate Plan covering a three year period which is updated on an annual rolling basis, and sets out the long term corporate aims and objectives of the Office together with its mission statement, and an annual Business Plan;
- key targets and performance measures have been established and incorporated into the Corporate and Business Plans. Progress against these targets and performance measures is reported to the sponsoring unit at the Lord Chancellor's Department on a quarterly basis, and annually in my Annual Report to Parliament;
- identification of the main risks facing the organisation and assigning ownership of these risks to members of the Management Board;
- an annual facilitated workshop to review and keep up to date the record of risks facing the organisation and to provide risk awareness training;
- an internal audit function, provided by Moore Stephens Chartered Accountants, who have prepared a three year plan of work, which is subject to annual review;
- reports by the internal auditor, including an independent opinion on the adequacy and effectiveness of the Office's system of internal control together with recommendations for improvement;
- an Audit Committee, comprising my Management Board, other senior employees and an external independent member, which is attended by the external and internal auditors, and which considers reports on internal control prepared for it by the internal auditors;
- the Management Board confirm on a periodic basis that they have no financial interests in transactions with the Commissioner;
- a published fraud response plan and formalised security guidelines for staff; and
- a whistle-blowing policy for confidential reporting of staff concerns.

My Office is currently undertaking a significant IS/ IT Change Programme

which is always a major risk to any organisation. To control such risk a Change Programme Strategy Board comprising senior managers representing all aspects of the work of the Office, including Finance, has been in place from the commencement of the programme, which advises the Management Board of progress with the project. In addition internal audit work has been specifically targeted to review the progress of the Change Programme and reported to my Audit Committee.

During the year my Office has formulated our approach to equality, to ensure my compliance with the requirements of the Race Relations (Amendment) Act 2000. In addition the IS/IT Change Programme is overseeing the development of an electronic document and records management system, which we aim to implement by the Government's target date of 2004.

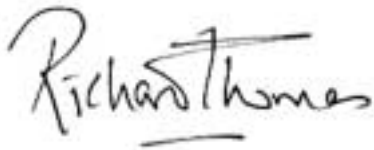
A revised Framework Document comprising a Management Statement and Financial Memorandum has been agreed with the Lord Chancellor's Department. The framework covers the operations, financing, accountability and control of my Office, and the conditions under which any government funds are provided to me.

Since my appointment on 30 November 2002, and in view of the growth and change of my Office over the last few years, I have undertaken a review of Corporate Governance within my Office, and I intend to strengthen internal control in the coming year by:

- re-constituting the Management Board with a re-defined role, and with the addition of up to three non-executive directors, meeting six times a year. The appointment process will be organised professionally, with open recruitment and with the appointments made by myself, a representative or nominee from the Lord Chancellor's Department and an independent person.
- establishing an Executive Team comprising the executive members of the Management Board and Head of IS, to meet most weeks.
- reconstituting the Audit Committee with revised terms of reference. Two non-executive directors will become members of the Committee, one of whom will be the Chairperson.
- improvements to the business planning process to articulate the detailed tasks and activities to be undertaken by each of the teams with my Office during the current Financial Year.

I am also proposing that the role and membership of the Senior Management Group will be reviewed as a further step of my Governance Review. Arrangements are needed to draw a sharper distinction between 'information exchange' and 'progress against plans' functions.

My review of the effectiveness of the system of internal control is informed by the work of the internal auditors and the senior managers who have responsibility for the development and maintenance of the internal control framework, and comments made by the external auditors in their management letter and other reports.



Richard Thomas
Information Commissioner
24 June 2003

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



I certify that I have audited the financial statements on pages 56 to 68 under the Data Protection Act 1998. These financial statements have been prepared under the historical cost convention as modified by the revaluation of certain fixed assets and the accounting policies set out on pages 59 to 61.

Respective responsibilities of the Information Commissioner and Auditor

As described on page 49, the Information Commissioner is responsible for the preparation of the financial statements and for ensuring the regularity of financial transactions. The Commissioner is also responsible for the preparation of the other contents of the Annual Report. My responsibilities, as independent auditor, are established by statute and guided by the Auditing Practices Board and the auditing profession's ethical guidance.

I report my opinion as to whether the financial statements give a true and fair view and are properly prepared in accordance with the Data Protection Act 1998 and directions made thereunder by the Lord Chancellor with the approval of the Treasury, and whether in all material respects the income and expenditure have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them. I also report if, in my opinion the Foreword is not consistent with the financial statements, if the Commissioner has not kept proper accounting records, or if I have not received all the information and explanations I require for my audit.

I read the other information contained in the Annual Report and consider whether it is consistent with the audited financial statements. I consider the implications for my certificate if I become aware of any apparent mis-statements or material inconsistencies with the financial statements.

I review whether the statement on pages 50 to 53 reflects the Commissioner's compliance with Treasury's guidance 'Corporate governance: statement on internal control'. I report if it does not meet the requirements specified by

Treasury, or if the statement is misleading or inconsistent with other information I am aware of from my audit of the financial statements.

Basis of Audit Opinion

I conducted my audit in accordance with United Kingdom Auditing Standards issued by the Auditing Practices Board. An audit includes examination, on a test basis, of evidence relevant to the amounts, disclosures and regularity of financial transactions included in the financial statements. It also includes an assessment of the significant estimates and judgements made by the Information Commissioner in the preparation of the financial statements, and of whether the accounting policies are appropriate to the Commissioner's circumstances, 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 error, or by fraud or other irregularity and that, in all material respects, the income and expenditure have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them. In forming my opinion I have also evaluated the overall adequacy of the presentation of information in the financial statements.

Opinion

In my opinion

- the financial statements give a true and fair view of the state of affairs of the Information Commissioner at 31 March 2003 and of the income and expenditure, total recognised gains and losses and cash flows for the year then ended and have been properly prepared in accordance with the Data Protection Act 1998 and directions made thereunder by the Lord Chancellor with the approval of Treasury; and
- in all material respects the income and expenditure have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them.

I have no observations to make on these financial statements.



John Bourn

Comptroller and Auditor General
26 June 2003

National Audit Office

157-197 Buckingham Palace Road
Victoria London SW1W 9SP

*Information Commissioner – Annual Report and Accounts 2003***Income and Expenditure Account for the year ended 31 March 2003**

		2002/2003		2001/2002	
	Note	£	£	£	£
Income					
Grant-in-aid	2	8,246,622		6,703,642	
Other Income	6	<u>62,035</u>		<u>11,606</u>	
			8,308,657		6,715,248
Expenditure					
Staff Costs	5	3,810,307		2,989,170	
Other Operating Costs	7	3,826,346		3,948,632	
Depreciation of Tangible Fixed Assets	8	<u>553,583</u>		<u>31,159</u>	
			(8,190,236)		(6,968,961)
Operating Surplus/(Deficit)			<u>118,421</u>		<u>(253,713)</u>
Fee Income	3		7,577,427		6,202,409
Interest Receivable			103,044		100,865
Notional Cost of Capital			(201,055)		(35,272)
Surplus for the year before appropriations			<u>7,597,837</u>		<u>6,014,289</u>
Notional Cost of Capital Reversal			201,055		35,272
Appropriations due to the Lord Chancellor			(7,742,506)		(6,314,880)
Retained Surplus/(Deficit) for the year			<u>56,386</u>		<u>(265,319)</u>

There were no recognised gains or losses other than reported above.

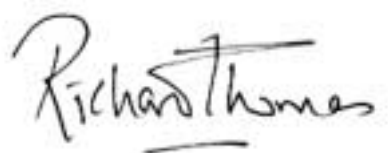
There were no material acquisitions or disposals in the year.

The notes on pages 59 to 68 form part of these accounts.

*The Certificate and Report of the Comptroller and Auditor General to the Houses of Parliament***Balance sheet as at 31 March 2003**

	Note	31 March 2003		31 March 2002	
		£	£	£	£
Fixed Assets					
Tangible fixed assets	8		5,952,435		1,573,057
Current Assets					
Debtors and prepayments	9	4,860,568		4,101,872	
Cash at bank and in hand	13	<u>234,854</u>		<u>1,146,533</u>	
		5,095,422		5,248,405	
Creditors – amounts falling due within one year	10	<u>(5,479,055)</u>		<u>(5,688,424)</u>	
Net Current Assets			(383,633)		(440,019)
Net Assets			<u>5,568,802</u>		<u>1,133,038</u>
Capital and Reserves					
Income and Expenditure Reserve	11		(383,633)		(440,019)
Other reserves	11		<u>5,952,435</u>		<u>1,573,057</u>
			<u>5,568,802</u>		<u>1,133,038</u>

The notes on pages 59 to 68 form part of these accounts.



Richard Thomas
Information Commissioner

24 June 2003

*Information Commissioner – Annual Report and Accounts 2003***Cashflow Statement for the year ended 31 March 2003**

	Note	2002/2003		2001/2002	
		£	£	£	£
Net cash inflow from operating activities	12		(937,694)		992,623
Returns on investments and servicing of finance					
Interest Received			103,044		100,865
Investing activities					
Payment to acquire tangible fixed assets			<u>(4,701,564)</u>		<u>(1,411,874)</u>
Net Cash Inflow before Financing			(5,536,214)		(318,386)
Financing					
Grant-in-aid for capital expenditure		4,701,564		1,411,874	
Fee Income received	3	8,233,185		5,104,962	
Less: Income Appropriated to the Lord Chancellor	4	<u>(8,310,214)</u>		<u>(5,154,753)</u>	
			<u>4,624,535</u>		<u>1,362,083</u>
(Decrease)\Increase in cash			<u>(911,679)</u>		<u>1,043,697</u>

The notes on pages 59 to 68 form part of these accounts.

Notes to the Accounts



1. Statement of Accounting Policies

1.1 Accounting Convention

These accounts have been prepared in accordance with an Accounts Direction issued by the Lord Chancellor, with the approval of the Treasury in accordance with paragraph (10)(1)(b) of schedule 5 to the Data Protection Act 1998.

These accounts shall give a true and fair view of the income and expenditure and cashflows for the financial year, and state the affairs as at the year-end. The accounts are prepared in accordance with Executive Non-Departmental Public Bodies Annual Reports and Accounts Guidance and other guidance which the Treasury has issued in respect of accounts which are required to give a true and fair view, except where agreed otherwise with the Treasury, in which case the exception is described in the notes to the accounts.

These accounts have been prepared under the historical cost convention, as modified by the inclusion of fixed assets at current cost. The Accounts meet the accounting and disclosure requirements of the Companies Act 1985 and the accounting standards issued or adopted by the Accounting Standards Board to the extent that those requirements are appropriate.

These accounts are prepared on a going concern basis.

1.2 Grant in Aid

Grant in Aid received for revenue expenditure is credited to income in the year to which it relates.

A proportion of the grant-in-aid received, equal to expenditure on fixed asset acquisitions in the period is taken to the Deferred Government Grant Reserve at the end of the financial year. The amount deferred is released back to the Income and Expenditure Account in line with depreciation charged. Losses on disposal of fixed assets are not debited to the Income and Expenditure Account, but are debited directly to the Deferred Government Grant Reserve.

1.3 Tangible Fixed Assets

Assets are capitalised as fixed assets if they are intended for use on a continuous basis, and their original purchase cost, on an individual basis, is £2,000 or more. Fixed Assets are valued at net current replacement cost by using

the **Price Index Numbers for Current Cost Accounting** published by the Office for National Statistics when the effect of revaluing assets is material.

Tangible Fixed Assets were not valued at net current replacement cost at 31 March 2003 as the effect is deemed as not material to the result reported.

1.4 Depreciation

Depreciation is provided on all fixed assets on a straight-line basis to write off the cost or valuation evenly over the asset's anticipated life. The principal rates adopted are:

Office fixtures	10 years
Office equipment	5 – 10 years
IT equipment and software	5 years
Assets under construction	nil

Depreciation rates are renewed annually to ensure that they remain appropriate for each asset.

1.5 Stock

Stocks of stationery and other consumable stores are not considered material and are written off to the Income and Expenditure as they are purchased.

1.6 Income Recognition

Fee income comprises notification fees in respect of notifications by data-controllers, under the Data Protection Act 1998 (implemented on 1 March 2000) and registration fees in respect of registrations by data-users under the Data Protection Act, 1984.

The notification fee is paid in advance for a period of 1 year, until 29 February 2000 registration fees were paid in advance for a period up to 3 years. A proportion of this income is therefore deferred and released back to the Income and Expenditure Account over the fee period.

Fee income is remitted regularly to the Lord Chancellor (prior to 1 April 2002 to the Secretary of State for the Home Department) and thus a prepayment is included within the Account in respect of income appropriated to the Lord Chancellor (prior to 1 April 2002 the Home Office) in advance of recognition of the income in the Income and Expenditure Account.

1.7 Notional Charges

In accordance with the Treasury guidance, **Executive Non-Departmental Public Bodies: Annual Reports and Accounts**, a notional charge for the cost of capital employed in the period is included in the Income and Expenditure Account along with an equivalent reversing notional income to finance the charge. The charge for the period is calculated using the Treasury's discount rate of 6% applied to the mean value of capital employed during the period.

1.8 Pensions

Pensions contributions are charged to the Income and Expenditure Account in the year of payment.

1.8 Operating Leases

Payments under operating leases are charged to the Income and Expenditure Account on a straight-line basis over the lease term, even if the payments are not made on such a basis.

1.9 Value Added Tax

Irrecoverable VAT is charged to the relevant expenditure category, or included in the capitalised purchase cost of fixed assets. Where output tax is charged or input tax is recoverable the amounts are stated net of VAT.

2. Grant-in-aid

	2002/2003	2001/2002
	£	£
Grant-in-aid drawn from the Lord Chancellor's Department	11,626,000	9,226,000
Grant in Aid prepaid by the Lord Chancellor's Department	1,000,000	(1,000,000)
Transfer to Deferred Government Grant Reserve in respect of fixed asset additions	(4,932,961)	(1,553,517)
Release of Deferred Government Grant in respect of depreciation charged	553,583	31,159
	<u>8,246,622</u>	<u>6,703,642</u>

3. Fee Income

Fees received in respect of notification fees were paid over to the Lord Chancellor (prior to 1st April 2002 to the Secretary of State for the Home Department).

Receipts in the period were as follows:

	Data Protection Act 1984	Data Protection Act 1998	2002/2003	2001/2002
	£	£	£	£
Deferred income at 1 April 2002	890,727	3,058,819	3,949,546	5,046,993
Cash received for fees	-	8,233,185	8,233,185	5,104,962
Deferred income at 31 March 2003	-	(4,605,304)	(4,605,304)	(3,949,546)
Fee Income from external fees	<u>890,727</u>	<u>6,686,700</u>	<u>7,577,427</u>	<u>6,202,409</u>

4. Appropriations

	2001/2002	2000/2001
	£	£
Cash received for fees (note 3)	8,233,185	5,104,962
Interest received	103,044	100,865
Other income	62,035	11,606
Home Office creditor at 1 April 2002	145,824	83,144
Lord Chancellor creditor at 31 March 2003	<u>(233,874)</u>	<u>(145,824)</u>
	<u>8,310,214</u>	<u>5,154,753</u>

Information Commissioner – Annual Report and Accounts 2003

5. Salaries

The average number of persons employed by the Commissioner during the year was as follows:

	2001/2002	2000/2001
	No.	No.
Corporate management	5	5
Senior staff	8	7
Other staff	176	142
Casuals and temporary agency staff	9	7
	<u>198</u>	<u>161</u>

The aggregate payroll costs of these persons were as follows:

	£	£
Wages and salaries	3,121,290	2,465,367
Social Security costs	192,601	162,001
Pension costs	403,340	305,209
Temporary agency staff	93,076	56,593
	<u>3,810,307</u>	<u>2,989,170</u>

Comparatives have been changed to include temporary agency staff, following new guidance.

The salary and pension entitlements of the Commissioner are paid directly from the Consolidated Fund and thus are not included above.

The Commissioner and Deputy Commissioners have consented to the disclosure of the salary and pension entitlements below:

	Age	Salary (£'000)	Real increase in pension at 60 (£'000)	Total accrued pension at 60 at 31 Mar 2003 (£'000)
Richard Thomas, <i>Information Commissioner</i> (30th November 2002 – 31st March 2003)	53	25 - 30	0 - 2.5	0 - 5
Elizabeth France, <i>Information Commissioner</i> (1st April 2002 – 30th September 2002)	53	40 - 45	0 - 2.5	30-35
Francis Aldhouse, <i>Deputy Commissioner</i>	57	65 - 70	0 - 2.5	10-15
Graham Smith, <i>Deputy Commissioner</i>	44	55 - 60	0 - 2.5	0 - 5

"Salary" comprises gross salary and any other allowance to the extent that it is subject to UK taxation.

Salaries (Continued)

Pension benefits are provided through the Civil Service pension arrangements. From 1 October 2002, civil servants may be in one of three statutory based "final salary" defined benefit schemes (classic, premium and classic plus). New entrants after 1 October 2002 may choose between membership of premium or joining a good quality "money purchase" stakeholder based arrangement with a significant employer contribution (partnership pension account).

(a) Classic Scheme

Benefits accrue at the rate of 1/80th of pensionable salary for each year of service. In addition, a lump sum equivalent to three years' pension is payable on retirement. Members pay contributions of 1.5 per cent of pensionable earnings. On death in service, the scheme pays a lump sum benefit of twice pensionable pay and also provides a service enhancement on computing the spouse's pension. The enhancement depends on length of service and cannot exceed 10 years. Medical retirement is possible in the event of serious ill health. In this case, pensions are brought into payment immediately without actuarial reduction and with service enhanced as for widow(er) pensions.

(b) Premium Scheme

Benefits accrue at the rate of 1/60th of final pensionable earnings for each year of service. Unlike classic, there is no automatic lump sum, but members may commute some of their pension to provide a lump sum up to a maximum of 3/80ths of final pensionable earnings for each year of service or 2.25 times pension if greater (the commutation rate is £12 of lump sum for each £1 of pension given up). For the purpose of pension disclosure the tables assume maximum commutation. Members pay contributions of 3.5 per cent of pensionable earnings. On death, pensions are payable to the surviving spouse or eligible partner at a rate of 3/8ths the member's pension (before any commutation). On death in service, the scheme pays a lump-sum benefit of three times pensionable earnings and also provides a service enhancement on computing the spouse's pension. The enhancement depends on length of service and cannot exceed 10 years. Medical retirement is possible in the event of serious ill health. In this case, pensions are brought into payment immediately without actuarial reduction. Where the member's ill health is such that it permanently prevents them undertaking any gainful employment, service is enhanced to what they would have accrued at age 60.

(c) Classic Plus Scheme

This is essentially a variation of premium, but with benefits in respect of service before 1 October 2002 calculated broadly as per classic.

Pensions payable under classic, premium, and classic plus are increased in line with the Retail Prices Index.

Pension benefits are provided through the Principal Civil Service Pension Scheme (PCSPS), an unfunded multi-employer defined benefit scheme in which the Information Commissioner is unable to identify its share of the underlying assets and liabilities. A full actuarial valuation was carried out as at 31 March 2003. Details can be found in the resource accounts of the Cabinet Office: Civil Superannuation (www.civilservice-pensions.gov.uk).

For 2002-2003, employers' contributions of £381,749 were payable to the PCSPS (2001/2002 £278,344) at one of four rates in the range 12 to 18.5 per cent of pensionable pay, based on salary bands. Rates will remain the same next year, subject to revalorisation of the salary bands. Employer's contributions are to be reviewed every four years following a full scheme valuation by the Government Actuary. The contribution rates reflect benefits as they are accrued, not when the costs are actually incurred, and reflect past experience of the scheme.

Salaries (Continued)

Agreement was reached to transfer the serving staff within The Data Protection Registrar's Staff Pension Scheme into the Principal Civil Service Pension Scheme with effect from 1 April 2000, one serving employee and the remaining past employees remain in The Data Protection Registrar's Staff Pension Scheme.

The Data Protection Registrar's Staff Pension Scheme is an unfunded by-analogy scheme (i.e. has identical provisions) to the PCSPS and paid pension benefits from grant-in-aid, to scheme members of £21,069 (2001/2002 - £20,736).

The remaining members of the Data Protection Registrar's Staff Pension Scheme were transferred to the PCSPS with effect from 1 April 2003. The most recent valuation of the pension liability was £858,770 as at 31 March 2002 calculated using the long-term underlying assumption that will be used in calculating the bulk transfer payment to the PCSPS. The pension liability has not been included in these accounts.

6. Other Income

	2002/2003	2001/2002
	£	£
Legal fees recovered	6,245	6,206
Contributions toward cost of International Conference	39,640	-
Other income	16,150	5,400
	<u>62,035</u>	<u>11,606</u>

7. Other Operating Costs

	2002/2003	2001/2002
	£	£
Rent and rates	633,827	550,046
Maintenance, cleaning, heating and lighting	129,335	216,435
Office supplies, printing and stationery	246,162	253,294
Carriage and telecommunications	133,180	137,558
Travel, subsistence and hospitality	310,537	233,084
Staff recruitment	105,236	86,916
Specialist assistance	135,189	255,954
Education and awareness	1,149,679	1,262,330
Legal costs	173,971	143,522
Staff training, health and safety	152,215	148,322
IT Services	637,663	643,599
Vehicle expenses	1,202	1,572
Audit fee	18,150	16,000
	<u>3,826,346</u>	<u>3,948,632</u>

Included in the above are operating lease payments for land and buildings totalling £511,883 (2001/2002 - £488,109).

8. Tangible Fixed Assets

	Equipment & Furniture	Information Technology	Assets Under Construction	Total
	£	£	£	£
Cost or Valuation				
At 1 April 2002	192,059	-	1,466,839	1,658,898
Additions	92,060	-	4,840,901	4,932,961
Transferred		2,530,181	(2,530,181)	-
Disposals	(7,090)	-	-	(7,090)
At 31 March 2003	<u>277,029</u>	<u>2,530,181</u>	<u>3,777,559</u>	<u>6,584,769</u>
Depreciation				
At 1 April 2002	85,841	-	-	85,841
Charged in year	47,547	506,036	-	553,583
Disposals	(7,090)	-	-	(7,090)
At 31 March 2003	<u>126,298</u>	<u>506,036</u>	<u>-</u>	<u>632,334</u>
Net Book Value				
At 31 March 2003	<u>150,731</u>	<u>2,024,145</u>	<u>3,777,559</u>	<u>5,952,435</u>
At 31 March 2002	<u>106,218</u>	<u>-</u>	<u>1,466,839</u>	<u>1,573,057</u>

Office equipment and furniture totalling £69,537 (2001/2002 - £69,587) has not been capitalised and is included within Other Operating Costs, as the individual costs were below the capitalisation threshold of £2,000.

Assets have not been re-valued in the year as the effect of revaluing assets makes no material difference to the results for the year or the financial position at the year end.

Assets under construction represent Information Technology projects not yet brought into service, comprising a casework management system £3,743,314 and a personnel system £34,245.

The net book value of Information Technology and Assets Under Construction includes £5,801,704 (2001/2002 - £1,276,633) on assets to which title belongs to a third party, provided under a managed service agreement as described in note 15.

9. Debtors

	31 March 2003	31 March 2002
	£	£
Fee income prepaid to the Lord Chancellor	4,605,304	3,949,546
Other prepayments	241,045	83,096
Other debtors	<u>14,219</u>	<u>69,230</u>
	<u>4,860,568</u>	<u>4,101,872</u>

Information Commissioner – Annual Report and Accounts 2003

10. Creditors; amounts falling due within one year

	31 March 2003	31 March 2002
	£	£
Trade creditors	169,053	543,349
Payroll	79,634	33,705
Accruals	18,150	16,000
Un-cleared fees and sundry receipts.	233,874	145,824
IS/IT retentions on assets under construction	373,040	-
Lord Chancellors Department – Deferred Grant-in-Aid	-	1,000,000
Deferred income	<u>4,605,304</u>	<u>3,949,546</u>
	<u>5,479,055</u>	<u>5,688,424</u>

11. Reserves

	Income & Expenditure Reserve	Deferred Government Grant Reserve	Revaluation Reserve	Total
	£	£	£	£
Balance at 1 April 2002	(440,019)	1,572,832	225	1,133,038
Retained surplus for the year	56,386	-	-	56,386
Grant deferred for additions	-	4,932,961	-	4,932,961
Release for depreciation	-	(553,583)	-	(553,583)
Balance at 31 March 2003	<u>(383,633)</u>	<u>5,952,210</u>	<u>225</u>	<u>5,568,802</u>

12. Reconciliation of Operating Surplus to Net Cash Inflow from Operating Activities

	2002/2003	2001/2002
	£	£
Operating surplus/(deficit) for the year	118,421	(253,713)
Depreciation provided in year	553,583	38,423
Release of deferred government grant	(553,583)	(38,423)
(Increase) in debtors relating to operating activities	(102,938)	(62,956)
(Reduction)/Increase in creditors relating to operating activities	<u>(953,177)</u>	<u>1,309,292</u>
Net cash inflow from operating activities	<u>(937,694)</u>	<u>992,623</u>

13. Cash at Bank and in Hand

	2002/2003	2001/2002
	£	£
Balance at 1 April 2002	1,146,533	102,836
Increase/(Decrease) in Cash	(911,679)	1,043,697
Balance at 31 March 2003	<u>234,854</u>	<u>1,146,533</u>
Commercial banks	234,183	1,146,230
Cash in hand	<u>671</u>	<u>303</u>
	<u>234,854</u>	<u>1,146,533</u>

14. Commitments under Operating Leases

At 31 March 2003 the Information Commissioner was committed to make the following annual payments in respect of operating leases expiring:

	Land and Buildings	
	31 March 2003	31 March 2002
	£	£
within one year	3,380	-
between two to five years	79,019	89,462
after five years	<u>381,875</u>	<u>379,180</u>
	<u>464,274</u>	<u>468,642</u>

The leases of land and buildings are subject to rent reviews.

15. Contingent Liabilities

The Information Commissioner has entered into a managed service agreement with Fujitsu Services Limited (formerly International Computers Limited) for the provision of Information Services. The contract term is seven years expiring in July 2004, with provision for a three year extension to July 2007. Expenditure under the contract in the year was £635,277 (2001/2002 - £503,431) for desktop and notification services, and £4,153,762 (2001/2002 - £1,311,905) for IS/IT development expenditure. The cost of cancelling the contract at 31 March 2003 would be £108,114 (31 March 2002 - £73,647).

16. Capital Commitments

At 31 March 2003 there were no capital commitments contracted for. (At 31 March 2002 – capital commitments of £597,096 were contracted for under the IT Services contract referred to in note 15 above).

17. Post Balance Sheet Events**Lord Chancellor's Department**

On 12 June 2003 the Government announced its intention to abolish the post of Lord Chancellor and for the work of the Lord Chancellor's Department to be taken over by a new Department for Constitutional Affairs. It is not anticipated that this constitutional change will materially affect the funding of the Information Commissioner's Office for the year ending 31 March 2004.

*Information Commissioner – Annual Report and Accounts 2003***18. Related Party Transactions**

The Information Commissioner confirms that he had no personal or business interests which conflict with his responsibilities as Commissioner.

The Lord Chancellor's Department is a related party to the Information Commissioner. During the year ending 31 March 2003 no related party transactions were entered into, with the exception of providing the Information Commissioner with grant-in-aid and collection of fee income and sundry receipts.

In addition, the Information Commissioner has had various material transactions with other central Government bodies. These transactions have been with the Central Office of Information (COI) and the Home Office Pay and Pension Service (HOPPS).

None of the key managerial staff or other related parties has undertaken any material transactions with the Information Commissioner during the year.

Appendix



Developments in Jurisprudence	70
Financial Matters	91
Output Measures and Performance Indicators	94
Our Annual Caseload	96

Developments in Jurisprudence

General Commentary

Last year's Annual Report incorporated, as an Appendix, a number of extracts from judgments in cases of direct relevance to our work. As well as domestic cases concerned with particular aspects of the Data Protection Acts 1984 and 1998 (DPA 84 and DPA 98) there have been decisions of both the domestic courts and the European Court of Human Rights in Strasbourg in the last year that are important to the developing jurisprudence in the area of 'privacy' law.

There is undoubtedly a body of 'privacy' law being developed by the higher courts in the context of cases involving high profile celebrities and their claims for rights to privacy as against the rights of newspapers and other media to publish articles about their private lives. This inevitably involves the courts in consideration of two competing human rights, contained in the European Convention on Human Rights and enshrined in UK law by the Human Rights Act 1998, the right to respect for private and family life (Article 8) and the right to freedom of expression (Article 10).

The cases referred to are set out in chronological order.

Case Extracts

Information Commissioner v. Islington London Borough Council

[2002] EWHC 1036 (Admin), Divisional Court (24 May 2002), Kennedy LJ and Hallett J

Hallett J

"22. Turning to the question of recklessness . . ., I am satisfied that there was sufficient evidence to meet the Galbraith test. The prosecution [the Commissioner] established that senior employees at the level of Director and or Assistant Director of Finance were aware of the council's duties under the Data Protection Act [1984] and were responsible for ensuring compliance with the Act. The fact that [a named council official] had left the council by the time the registration expired is in my view irrelevant. At all times the council remained under a duty to ensure compliance with the Act and to ensure that it had a proper system in place to effect renewal of the registration. It was reminded of the need to do so. The council as an ordinary prudent 'person', through its officers, would or should have known that any use of the data it held, in the absence of renewal, would be in contravention of the Act. The council as a body had either given no thought to the risk of causing the mischief which

section 5 [of the DPA 84] was designed to prevent or having recognised such a risk nevertheless went on to act as it did.

"23. In my judgment there was sufficient evidence that any use of data in November 1999 by a Council employee acting in the course of his or her employment must have been, at the very least, reckless on the part of the Council as a whole. I reject [the Council's] argument that the prosecution had to prove that the person who accessed the computer to send out the council tax summons to B acted recklessly. Such an approach would make it virtually impossible to hold a large organisation to account for the unlawful use of data knowingly or recklessly. It would effectively defeat the purpose of subsection (2) [of section 5 of the DPA 84]. It is highly unlikely that any of the directing minds of a body corporate would be personally responsible for day to day administration such as sending out letters or arranging for the issue of a summons. It is also unlikely that the person responsible for doing so, at a lower level, would have any knowledge of the council's status as far as registration [under the DPA 84] is concerned. In my judgment the knowledge and actions of the directing minds of a corporate body must be taken together with the actions of those to whom administrative functions are delegated for the purposes of the section."

Lord Justice Kennedy

"28. In my judgment if a corporate body such as this council fails to renew a registration it can reasonably be inferred that it is aware of its omission, and that inference is reinforced when, as in this case, the council, through the medium of its relevant official, is specifically reminded of the need to renew and subsequently of the failure to do so. If thereafter the council, as a result of the actions of some other officer, acting within the normal course of his or her employment, uses data which should not be used when unregistered then, as it seems to me, the council must be found to have knowingly or recklessly contravened the prohibition on such user. The Deputy District Judge rightly accepted that 'a body such as the defendant borough was capable of acting knowingly or recklessly', and in my judgment there was ample evidence to show that, at least in relation to the B matter, this borough did so."

Case commentary

This case was referred to in last year's Annual Report, in a footnote to the prosecutions table. The local authority were charged by the Commissioner with seven counts of knowingly or recklessly "using" personal data for purposes not contained in their register entries contrary to sections 5(2), 5(5)

and 19(2) of the DPA 84. At the Magistrates Court the local authority were acquitted of all 7 offences. The Commissioner lodged an appeal by way of case stated which was heard by the Divisional Court (not the Court of Appeal as mistakenly referred to in last year's report) on 2 May 2002. On 24 May 2002 the Court gave its judgment ordering that the appeal be allowed in respect of one charge and the case was remitted to the Magistrates Court. The Council there entered a guilty plea and were fined £3,000 and ordered to contribute £2,350 to prosecution costs. Although concerned with offences under the DPA 84 we believe the judgment will provide useful authority in relation to issues of corporate responsibility. The case established an important principle that the knowledge and actions of the directing minds of a corporate body must be taken together with the actions of those to whom administrative functions are delegated in determining criminal responsibility for the actions of a corporate body.

Lord Ashcroft v. (1) Attorney-General (2) Department for International Development [2002] EWHC 1122 (QB), High Court (31 May 2002), Gray J.

"26. I accept that the only private law right to damages which is conferred by the [Data Protection Act] 1984 . . . arises under section 23 [right to compensation for loss, destruction or unauthorised disclosure of personal data]. . . . But I do not accept that it is open to Lord Ashcroft in the present proceedings to claim damages for breach of the principles. Any such breach is a matter which by the terms of the 1984 Act is for the [Data Protection] Registrar. . . .

"27. . . . [in respect of the allegation that an alleged disclosure was contrary to the eighth principle of the DPA 84, requiring appropriate security measures to be taken against unauthorised access to or alteration, disclosure or destruction of personal data] I accept the argument . . . that, whilst the fact of disclosure may be evidence of a failure to take security precautions, disclosure cannot of itself amount to a breach of the obligation to take security measures.

"29. The position under the [Data Protection Act] 1998 . . . is entirely different: there is a free-standing duty on data [controllers] under section 4(4) to comply with the principles which are set out in Schedule 1, Part I. By section 13 breach of those principles does sound in damages, as does breach of any of the requirements of the 1998 Act. Section 14 confers a right to rectification, blocking, erasure or destruction of personal data. Although enforcing compliance with the principles is for the Commissioner, it is clear that [his] jurisdiction is

non-exclusive so far as claims for damages by data subjects are concerned.

"35. As I have already held, a right to damages does arise under the 1998 DPA for breach of the principles contained therein. The Claimant alleges that the disclosure of the documents amounted to a breach of the seventh principle [of the DPA 98], which requires data [controllers] to take appropriate technical and organisational measures against disclosure. I disallow this part of the pleading for the same reason I disallowed the [DPA 84 eighth principle] allegation [see above] . . . , namely that disclosure may be evidence of breach of the obligation to take such measures but cannot in itself amount to such a breach."

P. v. David Wozencroft [2002] EWHC 1724 (Fam), High Court (15 July 2002), Wilson J.

"... subsection [(9) of section 7 of the DPA 98] confers upon the court a discretion as to whether to order the disclosure of . . . documents. I consider it of extreme significance that, even though s.7(1) speaks in terms of entitlement to disclosure on the part of the subject of data, the court is given a discretion, by the use of the word 'may' rather than any word such as 'must' or 'shall', as to whether to make the order.

"It is also important to note that an analogous discretion is reflected in the terminology of s.14 [of the DPA 98]... s.14 is engaged only if the court is satisfied that personal data are inaccurate; and, even then, a discretion arises as to whether to order their rectification.

"... relief is discretionary and . . . in the exercise of the discretion the existence of a more appropriate forum for the articulation of these issues would be a decisive factor. . . . no litigation, whatever the statute or other law upon which it be cast, is immune from liability to be struck out as an abuse of process . . .

"... I say with confidence that it is an abuse of process to use later proceedings in order to ventilate challenges which were clearly apt to be ventilated in earlier proceedings in which the claimant was a party."

Case commentary

The claimant in this case (P) sought to challenge the accuracy of reports prepared by the defendant (a consultant child psychiatrist) for the court in the course of previous proceedings under the Children Act 1989, which had concluded. P sent a subject access request to the defendant. P later issued proceedings under sections 7 and 14 of the DPA 98 seeking, respectively, 'disclosure' of all the documents held by the defendant of which P was the subject, and 'rectification, blocking, erasure or destruction' of personal data in the two reports on the basis they were 'inaccurate'. The purpose of the High Court hearing was to decide, as a preliminary issue, whether, as a matter of law, either or both of the claims could succeed. The parties agreed that the defendant no longer held any documents which had not been disclosed to P and so this element of the claim was dismissed. This left the issue of the section 14 claim to be determined. The judge dismissed this part of the claim as an abuse of process of the court. In ruling thus the learned judge effectively adopted the defendant's submission that the DPA 98 "is not intended to provide a vehicle to enable experts' reports in litigation to be challenged after that litigation has been brought to a conclusion."

The case is of some practical interest in that whilst this claimant may have exercised his right to go to court under the DPA 98, the court made it clear that such right does not exist in isolation and will be considered by the court, like any other claim, subject to the procedural rules of the courts. The rights in the DPA are unlikely to be available to litigants wishing, in effect, to 're-open the old wounds' of previous litigation. In our experience of compliance work it is quite common for people to resort to remedies that may be available under the DPA 98 in relation to cases that have already been the subject of previous litigation. This case suggests that the courts are less likely to entertain such claims where an opportunity to challenge the same personal information has been afforded the individual in an earlier claim.

R (on the applications of S & Marper) v. Chief Constable of South Yorkshire [2003] 1 All ER 148, Court of Appeal (12 September 2002) – subject to appeal to the House of Lords (case pending)

Lord Woolf CJ

"2. . . . The cases are of particular interest because in this country the public are particularly sensitive about the State unnecessarily retaining personal information about members of the public or requiring members of the public to provide information to the State without good reason. An example of the latter sensitivity being the controversy created by any proposal to require individuals to carry identity cards.

"3. On these appeals, it is the retention of fingerprints and DNA samples which were taken during the course of criminal investigations if the prosecutions of the individuals from whom they were taken are either discontinued or result in an acquittal that is challenged. . . .

"32. The extent to which the retention of material of this nature is regarded as interfering with the personal integrity of the individual, as it seems to me, depends very much on the cultural traditions of a particular State. So far as this jurisdiction is concerned it is my view that fingerprints and DNA samples are material which is regarded as being personal to the individual from whom it is taken and so requires legal justification before it can be retained. . . .

"33. While I am satisfied that Article 8(1) applies to the retention, the extent of the interference with that Article is important when considering the next issue, namely whether the interference can be justified under Article 8(2). As to this I do not regard the interference as being significant. . . .

"34. Nonetheless, while not substantial, the interference is still real. There are no doubt a rainbow of reactions which are possible to intrusions of this nature, but at least for a substantial proportion of the public there is a strong objection to the State storing information relating to an individual unless there is some objective justification for this happening. The objection to the storage is reflected in the appreciative public response to novels such as Aldous Huxley's "Brave New World" and George Orwell's "1984". As to the persuasive decisions of the Commission, it has to be remembered that just as in the appropriate circumstances a margin of appreciation has to be extended for any shortcomings in this jurisdiction in relation to observing the ECHR, so there can be situations where the standards of respect for the rights of the individual in this jurisdiction are higher than those required by the ECHR. There is nothing in the Convention setting a ceiling on the level of respect, which a jurisdiction is entitled to extend to personal rights. In this jurisdiction I would not expect a court to necessarily follow the decision of the Commission in *Reyntjens v. Belgium* (1992) 73 DR 136 that:

". . . The obligation to carry an identity card and to show it to the police when requested to do so does not as such constitute an interference in a person's private life within the meaning of Article 8 of the Convention". (Paragraph 23)

"35. It is also to be noted . . . that the information relating to the genetic make up of an individual which can be obtained from a DNA sample is continually expanding.

"53. The arguments raised by Liberty have been carefully considered . . . I accept that the information, which can be derived from a sample of DNA, is growing rapidly. So are the purposes for which the information can be used. Information may already, and certainly in the future will be capable of being obtained from samples which goes well beyond the prevention and detection of crime as now understood. However, the Chief Constable is not contemplating using samples for purposes other than the prevention and detection of crime in the narrow sense, that is in exactly the same way as fingerprints can be used, for identifying or excluding an individual from responsibility for a crime. In its consideration of a case the EC[t]HR is careful to confine its judgment to the facts of the case which is before it and, in my judgment, we should adopt the same course and not try to anticipate events.

"54. The police can make mistakes and act unlawfully but it does not seem to me that the risk that this could happen can affect the outcome of this appeal. The court must assume that the police will act lawfully until the contrary is shown. If the developments of science expand the purposes for which DNA can be used then the Chief Constable must use his discretion to ensure that the DNA is not used for any purpose not authorised by Parliament. He has ample discretion not to allow samples to be used for purposes contrary to Article 8 and Article 14. there is no need to read the statutory provisions in a restricted manner. If in the future a question arises as to the lawfulness of the use of samples in a manner that is not now contemplated that will have to be dealt with when the problem arises."

Naomi Campbell v. MGN Limited [2003] 1 All ER 224, Court of Appeal (14 October 2002) – subject to appeal to the House of Lords (case pending)

Lord Phillips MR

"8. These are the first proceedings in which interpretation of the Data Protection Act [1998] has fallen for determination.

"40. . . . When Lord Woolf [CJ] [in the case of *A. v. B* (a company) [2002] 2 All ER 545] spoke of the public having 'an understandable and so a legitimate interest in being told' information, even including trivial facts, about a public figure, he was not speaking of private facts which a fair-minded person would consider it offensive to disclose. That is clear from his subsequent commendation of the guidance on striking a balance between Article 8 and Article 10 rights provided by the Council of Europe Resolution 1165 of 1998.

"43. The courts are in the process of identifying, on a case by case basis, the principles by which the law of confidentiality must accommodate the Article 8 and Article 10 rights. One principle, . . . is that, where a public figure chooses to make untrue pronouncements about his or her private life, the press will normally be entitled to put the record straight.

"61. . . . In this jurisdiction both protection of privacy by expanding the scope of breach of confidence and the public interest defence of qualified privilege in defamation are in the course of development We do not believe that the same test of public interest applies to justify publication in these two very different torts.

"70. The development of the law of confidentiality since the Human Rights Act came into force has seen information described as 'confidential' not where it has been confided by one person to another, but where it relates to an aspect of an individual's private life which he does not choose to make public. We consider that the unjustifiable publication of such information would better be described as breach of privacy rather than breach of confidence.

"72. The Data Protection Act 1998 ('the Act') regulates the processing of information about individuals. Section 13 of the Act entitles, in specified circumstances, an individual who suffers damage or distress by reason of contravention of the Act, to recover compensation. Morland J. [the judge at first instance] held that Miss Campbell had established an entitlement to damages under this section. He described his path to this conclusion as weaving his way through a thicket, and the Act is certainly a cumbersome and inelegant piece of legislation. It was passed to give effect to Directive 95/46/EC of the European Parliament and the Council on 'the protection of individuals with regard to the processing of personal data and the free movement of such data' ('the Directive'). The Act largely follows the form of the Directive. It replaces the Data Protection Act 1984.

"73. The Directive was a response to the greater ease with which data can be processed and exchanged as a result of the advances in information technology. Foremost among its aims is the protection of individuals against prejudice as a consequence of the processing of their personal data, including invasion of their privacy.

"97. In interpreting the Act it is appropriate to look to the Directive for assistance. The Act should, if possible, be interpreted in a manner that is consistent with the Directive. Furthermore, because the Act has, in large measure, adopted the wording of the Directive, it is not appropriate to look for the precision in the use of language that is usually to be expected from the Parliamentary draftsman. A purposive approach to making sense of the provisions is called for.

"98. The preamble to the Directive runs to 72 recitals. A number of these refer to the right to privacy, of which the following is typical:

"(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community."

"101. The definition of 'processing' in the Directive and the Act alike is very wide. 'Use of the information or data' and 'disclosure of information or data by transmission, dissemination or otherwise making available' are phrases, given their natural meaning, which embrace the publication of hard copies of documents on which the data has been printed. Is such meaning consistent with an interpretation which gives effect, in a sensible manner, to the objects of the Act?

"103. The Directive and the Act define processing as 'any operation or set of operations'. At one end of the process 'obtaining the information' is included, and at the other end 'using the information'. While neither activity in itself may sensibly amount to processing, if that activity is carried on by, or at the instigation of, a 'data controller', as defined, and is linked to automated processing of the data, we can see no reason why the entire set of operations should not fall within

the scope of the legislation. On the contrary, we consider that there are good reasons why it should.

"104. While an individual may reasonably find it objectionable that another should record and hold personal data about himself, the greater invasion of privacy, damage and distress is likely to be caused when that information is made public. . . . If publication were not treated as part of a 'processing operation' [Article 23 of the Directive] would be deprived of much of its force.

"105. Section 13 of the Act gives effect to Article 23. . . . Once again, if [the] provisions [of section 13] are to be effective, publication must be treated as part of the operations covered by the requirements of the Act.

"106. Accordingly we conclude that, where the data controller is responsible for the publication of hard copies that reproduce data that has previously been processed by means of equipment operating automatically, the publication forms part of the processing and falls within the scope of the Act.

"111. We accept that [Recital 37 and Article 9 of the Directive] must inform the interpretation of s.32 [of the DPA 98]. They do not, however, suggest that exemptions will only be appropriate if their application is limited to the period prior to publication.

"119. . . . it would seem totally illogical to exempt the data controller from the obligation, prior to publication, to comply with provisions which he reasonably believes are incompatible with journalism, but to leave him exposed to a claim for compensation under s.13 the moment that the data have been published.

"120. For these reasons we have reached the conclusion that, giving the provisions of the sub-sections [(1) to (3) of section 32] their natural meaning and the only meaning that makes sense of them, they apply both before and after publication.

"123. . . . the requirements of the Act, in the absence of s.32, would impose restrictions on the media which would radically restrict the freedom of the press. . . .

"129. Under s.32(1) it is the data which is exempt from the provisions of the Act specified in sub-section (2). The Act only applies in relation to data. If, as we have held, the Act applies to publication, as part of the processing operation, it does so because the information published remains 'data', as defined by the Act. Where, by reason of s.32 the data becomes exempt as a result of the reasonable belief of the journalist that the publication *will be* in the public interest, the data remains subject to that exemption thereafter.

"130. It follows that, contrary to the findings of Morland J., the Appellants were entitled to invoke the provisions of s.32 in answer to Miss Campbell's claim.

"136. We do not consider that it would have been reasonably practicable to comply with the provisions of the data protection principles while at the same time making the publications in question. It follows that the Appellants have made good their contention that the three conditions of exemption under s.32 were satisfied.

"137. For these reasons we find that there was no infringement by the Appellants of the Act."

Case commentary

In this case the Court of Appeal has confirmed and clarified various 'routine' matters of interpretation relating to both Directive 95/46/EC and the DPA 98, making various helpful passing comments on the general ambit of these provisions. The Court confirmed that the definition of 'processing' in the DPA 98 is "very wide" and that "publication must be treated as part of the operations covered by the requirements of the Act." Some legal commentators have characterised the Court of Appeal's judgment in this case as a denial of any right to privacy. In the Commissioner's view this is quite wrong; rather, the Court are still feeling their way in that direction. On the central question of where the law stands on the "Article 8 v. Article 10 issue", the courts are, in the Commissioner's view, still slowly and carefully moving towards establishing a common law concept of privacy within, alongside or, possibly, outside the realms of the law of confidence. In an appropriate case, on the particular facts, the courts will almost inevitably find there to be a 'breach of privacy' as opposed to a 'breach of confidence'.

But what will be an appropriate case? What will be the particular facts? How will the case by case approach work? What will be an 'unjustifiable

publication'? At this stage the Commissioner's prediction is that the courts will move further down this road in a case involving a genuine private person, not a celebrity or other public figure.

The Court of Appeal clearly adopted a wide approach to the "special purposes" exemption at section 32 of the DPA 98, making it clear that it can apply after, as well as before, publication. The Commissioner would though want to make it clear that the exemption does not provide unlimited exemption from the whole Act for the media. This is very clearly not the case. The section 32 exemption only applies in relation to particular provisions of the Act, and only to the extent that there is a reasonable belief that compliance with any such provision would prejudice any of the 'special purposes', including journalistic purposes. It does not provide carte blanche for the media.

The Commissioner notes that the Court of Appeal's judgment is currently the subject of an appeal to the House of Lords which is not expected to be heard before the publication of this Report. The Commissioner awaits with interest their Lordships' judgment in this important case.

Durant v Financial Services Authority, Edmonton County Court (24 October 2002), HHJ Zeidman QC – subject to appeal to the Court of Appeal (case pending)

"I . . . reach the conclusion that it is not necessary or appropriate for me to have regard to [Parliamentary] material in reaching my conclusion. I do not need *Pepper v. Hart* in relation to the problem that has arisen in this case. . . .

"I am at this stage concerned with information that is recorded in paper files, not on computer, and I have to look, although I am adopting a purposive approach, at the wording and the definition. Data means in this context information which in (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. In order to understand the phrase 'relevant filing system' I need to look at the definition of that phrase on the next page of the statute where I am told it means:

'Any set of information relating to individuals, to the extent that although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose the set is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible.'

"I need to break that down into separate questions in order to determine whether the material in issue in this case falls within the definition:

"Question 1. Is the material a set of information relating to an individual?

"Question 2. Is the material structured either by reference to individuals or by reference to criteria relating to individuals?

"Question 3. Is it structured in such a way that specific information relating to a particular individual is readily accessible?

"The strict requirements of the definition can be understood if one remembers the context into which this rule is placed. Most of the provisions in this Act deal with computer information but if one is able to arrange material in a non-computer form but in a form which apes the processing of a computer then the information is likely to be caught by the definition. The Act says that the fact that the information is not processed by means of operating automatically in response to instructions given for that purpose will not prevent the material coming within the definition of a relevant filing system if it is structured in the way anticipated by the statute, so I need to concentrate on the structure. . . .

". . . I have reached the conclusion that in law the documents sought [save one] do not come within the obligation of disclosure as contained in the strict wording of the Act, but for the sake of completeness I should deal with the further submission directed to the exercise of discretion. Even if the respondents had failed to comply with their duty under the Act, and of course I have ruled that they have complied with their duty, but even if they had not done so it would not necessarily follow that I should make an order for disclosure of the material. S.7(9) of the Act provides that:

'If a court is satisfied on the application of any person who has made a request under the foregoing provisions of this section that the data controller has failed to comply with the request in contravention of these provisions the court may order him to comply with the request.'

"The use of the word 'may' that I have emphasized in this context is significant. It says 'may' and not 'shall'. It gives me a discretion."

Case commentary

The learned judge in this case has applied a restrictive interpretation on the scope of the definition of 'relevant filing system' in the DPA 98. The Commissioner has propounded the view that provided information is structured either by reference to individuals or by reference to criteria relating to individuals, it is quite possible for information within that structure to be readily accessible, even where the information is stored in date order.

At the time of this Report going to print the Commissioner understands that this decision is being appealed by Mr Durant. Pending the outcome of any such appeal, the Commissioner's view remains unaltered and he will continue to make assessments in accordance with that view.

However, in any case where the interpretation of 'relevant filing system' is a central issue, the Commissioner will defer any decision as to whether to institute enforcement proceedings until the outcome of any appeal is known. The Commissioner will reconsider his interpretation of the definition of 'relevant filing system' in the light of any appeal ruling and, in doing so, will consider whether the particular circumstances of this case are distinguishable from the general position.

Re Terence Patrick Ewing, [2002], High Court (Case No: IHQ/02/0198) (20 December 2002), Davis J.

"40. In my view the Information Tribunal, dealing with appeals under section 28 of the [Data Protection Act] 1998 . . . , is a court within the ambit of s.42 of the [Supreme Court Act] 1981 . . .

"43. . . . The nature of the proceedings before the Information Tribunal (being proceedings which at least relate to the rights of subjects) is such, given the functions and procedures of the Information Tribunal, that they are civil proceedings.

51. . . . It is the judicial function and duty of the Court, on applications under s.42(3) [of the Supreme Court Act 1981], first to decide whether it is satisfied that the proposed proceedings in question are not an abuse of the court concerned and whether there are reasonable grounds for the proceedings. That is a precondition to the grant of leave. Were it otherwise the whole policy underlying s.42 could be defeated. I thus must make such an assessment.

"53. The [section 28 DPA 98] certificate [relating to the work of the Security Service signed by the Home Secretary on 10 December 2001] is long and complex. I had a considerable amount of sympathy with Mr Ewing's complaint that it was difficult to follow. However, in fairness it should be said that it deals with complex issues: and its effect does reveal itself after more than one reading. The certificate itself is a general certificate: that is to say, it is designed (for obvious practical reasons) for use in cases other than just Mr Ewing's (cf s.28(3)). . . .

"56. The Reasons document referred to in paragraph 2 of the certificate is available to the public and was supplied to Mr Ewing. It is a 12 page document, written in clear and plain English. It sets out the background to the 1998 Act; the functions of the Security Service, and the need for secrecy in the national interest; the need for a policy of 'neither confirm nor deny' (NCND) with regard to information relating to the Security Service; the controls over, and supervision of, the Security Service; and the reasons for, and the explanations as to the form and scope of, the certificate.

"58. In the light of [the] ruling [of the Information Tribunal (National Security Appeals) dated 1 October 2001 in the case of Mr Norman Baker MP's appeal against the previous certificate, dated 22 July 2000, issued under section 28 of the DPA 98 by the Home Secretary in respect of the Security Service], the form of the certificate was changed, to that provided to Mr Ewing. It is self evident . . . that the criticisms of the Information Tribunal as to the previous form of certificate, as identified in the **Baker** case, have been addressed. The certificate now requires that, on each individual application, data is not to be exempt if the Security Service, after consideration of such request, determines that adherence to the NCND policy for the purposes of s.7(1)(a) is not required for the purpose of safeguarding national security or that for the purposes of s.7(1)(b)(c)(d), non-communication of such data is not required for the purpose of safeguarding national security. It is to be noted that the certificate does not give the Security Service a discretion as to whether or not to

examine and consider each individual request: it is required to do so. Section 10 of the Reasons (in plain English) also spells that out.

"60. . . . In my view, a general NCND policy, in response to requests for personal data, including as to the existence (or non-existence) of personal data, is in principle justifiable and cannot be criticised as unreasonable or unnecessary. So much, indeed, was accepted by the information Tribunal in the **Baker** case itself. It could clearly be very damaging to national security if individuals or organisations could know that data was held by the Security Service on him or them (or, indeed, if they could know that no such data was held). The underlying reasoning is obvious and is summarised in section 5 of the Reasons document incorporated by the certificate itself. The vice, identified by the decision in **Baker**, was to apply such policy inflexibly, without any regard to the possibility, in an individual case, that exemption was not required in the interests of national security. That vice has been cured by the revised form of certificate. . . .

"67. I would like to add one observation. In those cases where the Security Service proposes to rely on the current certificate and, in particular, to seek exemption in respect of s.7(1) of the 1998 Act, I would suggest that it might be considered desirable (in the ordinary case, at any rate) that the letter so notifying the individual applicant expressly includes the words in plain English to the effect that individual consideration has been given to his particular request. It will be understood that such a statement cannot lawfully be made, or the exemption of s.7(1) contained in the certificate lawfully invoked, unless that has indeed been the case."

Case commentary

This case concerned an application made by Mr Ewing for a declaration that he did not require leave of the High Court to pursue an appeal before the Information Tribunal (National Security Appeals) under section 28 of the DPA 98 as a result of him being subject to a "Vexatious Litigant Order" made in 1989 under section 42 of the Supreme Court Act 1981 ('section 42'). Section 42 prevents persons subject to such an order bringing civil proceedings before a court without first getting leave from the High Court to do so.

The High Court judge ruled that a section 28 appeal to the Tribunal constitutes civil proceedings, and that the Tribunal is a court for the purposes of section 42. In deciding whether or not to grant leave to Mr Ewing, the learned judge considered whether there were reasonable grounds for the

proceedings in question (i.e. the section 28 appeal). The learned judge found there were no such grounds and refused to give leave. This involved his consideration of the certificate under appeal and it will be interesting to see the extent to which the Tribunal take into account the learned judge's ruling in respect of other appeals against the same certificate, or other certificates issued since the Tribunal's ruling in the **Baker** case. There are two Tribunal rulings awaited at the time this report was being compiled.

Peck v. The United Kingdom [2003], European Court of Human Rights (Application No. 44647/98) (28 January 2003)

"59. The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life (see, for example *Herbecq and Another v. Belgium* . . .). On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations.

"60. . . . the Court notes that [Mr Peck] did not complain that the collection of data through the CCTV camera monitoring of his movements and the creation of a permanent record of itself amounted to an interference with his private life. . . . Rather he argued that it was the disclosure of that record of his movements to the public in a manner in which he could never have foreseen which gave rise to such an interference.

"61. In this respect, the Court recalls the *Lupker and Friedl* cases decided by the Commission which concerned the unforeseen use by the authorities of photographs which had been previously voluntarily submitted to them. . . . In those cases, the Commission attached importance to whether the photographs amounted to an intrusion into the applicant's privacy (as, for instance, by entering and taking photographs in a person's home), whether the photograph related to private or public matters and whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public.

"62. [In the case of Mr Peck] the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation . . . and to a degree surpassing that which the applicant could possibly have foreseen

"63. Accordingly, the Court considers that the disclosure by the Council of the relevant footage constituted a serious interference with the applicant's right to respect for his private life."

Jean F Jones v. University of Warwick [2003], Court of Appeal (4 February 2003) Woolf CJ

"1. The issue which this appeal raises is whether, and if so when, a defendant to a personal injury claim is entitled to use as evidence a video of the claimant which was obtained by filming the claimant in her home without her knowledge after the person taking the film had obtained access to the claimant's home by deception.

"2. . . . the issue on the appeal requires this court to consider two competing public interests: the interests of the public that in litigation, the truth should be revealed and the interests of the public that the courts should not acquiesce in, let alone encourage, a party to use unlawful means to obtain evidence.

"21. It is not possible to reconcile in a totally satisfactory manner, the conflicting public policies . . . in this case. . . .

"23. If the conduct of the insurers in this case goes uncensored there would be a significant risk that practices of this type would be encouraged. This would be highly undesirable, particularly as there will be cases in which a claimant's privacy will be infringed and the evidence obtained will confirm that the claimant has not exaggerated the claim in any way. This could still be the result in this case.

"27. As the Strasbourg jurisprudence makes clear, the Convention does not decide what is to be the consequence of evidence being obtained in breach of Article 8 This is a matter, at least initially, for the domestic courts. Once the court has decided the order, which it should make in order to deal with the case justly, . . . then it is required or it is necessary for the court to make that order. Accordingly if the court could be said to have breached Article 8.1 by making the order which it has decided the law requires, it would be acting within Article 8.2 in doing so.

"28. . . . The court must try to give effect to what are here the two conflicting public interests. The weight to be attached to each will

vary according to the circumstances. The significance of the evidence will differ as will the gravity of the breach of Article 8, according to the facts of the particular case. The decision will depend on all the circumstances."

Case commentary

This is an important case on the contentious issue of private video surveillance by defendant insurers in personal injury cases. Although such practice was roundly criticised by the Lord Chief Justice in this case as being "improper and not justified" the court ruled that the evidence obtained in this way in this case should not be excluded from the trial of the matter. The court was mindful of the 'overriding objective' of the Civil Procedure Rules 1998 (which is to enable the courts 'to deal with cases justly'). The court had to consider the effect of its decision on litigation generally and not just the case before it. To discourage conduct of this nature the court ordered the insurers to pay the costs of having the issue determined and said it would indicate to the trial judge that the insurer's conduct should be taken into account when considering the appropriate order for costs at the trial.

Douglas and Others v. Hello! Ltd and Others [2003] EWHC 786 (Ch), High Court (11 April 2003) Lindsay J.

"Privacy

"229. . . . So broad is the subject of privacy and such are the ramifications of any free-standing law in the area that the subject is better left to Parliament which can, of course, consult interests far more widely than can be taken into account in the course of ordinary inter partes litigation. A judge should therefore be chary of doing that which is better done by Parliament. That Parliament has failed so far to grasp the nettle does not prove that it will not have to be grasped in the future. The recent judgment in *Peck –v- United Kingdom* in the ECHR, given on the 28th January 2003, shows that in circumstances where the law of confidence did not operate our domestic law has already been held to be inadequate. That inadequacy will have to be made good and if Parliament does not step in then the Courts will be obliged to. Further development by the Courts may merely be awaiting the first post-Human Rights Act case where neither the law of confidence nor any other domestic law protects an individual who deserves protection. A glance at a crystal ball of, so to speak, only a low wattage suggests that if Parliament does not act soon the less satisfactory course, of the Courts creating the law bit by bit at the

expense of litigants and with inevitable delays and uncertainty, will be thrust upon the judiciary. But that will only happen when a case arises in which the existing law of confidence gives no or inadequate protection; this case now before me is not such a case and there is therefore no need for me to attempt to construct a law of privacy and, that being so, it would be wrong of me to attempt to do so.

"Data Protection Act 1998

"230. There is a full analysis of the relevant provisions of the Act in Campbell supra at paragraphs 72-138, which, fortunately, make an understanding of the Act easier than do the unvarnished provisions of the Act itself. At the risk of my construing the authority rather than the Act itself, I find, after reading Campbell, that all three Hello! Defendants can be taken to be a data controller, that the unauthorised pictures represent personal data and that publication of them in England is to be treated as part of the operations covered by the requirements of the Act. That is because when a data controller is responsible for the publication of hard copies that reproduce data that has previously been processed by means of equipment operated automatically, the publication forms part of the process and falls within the scope of the Act. The hard copies here were, of course, the copies of Hello! magazine

"231. That there had been such processing by equipment operating automatically appears because such processes were used in the transmission by ISDN Line from California to London, in the calling up of the pictures on to a screen in London . . . , in [the] transmission of them to Madrid by ISDN Line, in the taking out from unauthorised photographs of the defects that one or more of the earlier processes had introduced into them, in the transmission from Hola's office in Madrid to the printers and the processes used in the course of preparation for and in the course of printing. I am told that there was also publication of the unauthorised photographs on a Hello! Website. The exemption given in respect of the processing of personal data for journalistic purposes, the exemption which the Court of Appeal held to apply in Campbell, does not apply in the case before me because it depends, inter alia, on the data controller reasonably believing that publication would be in the public interest. I have had no credible evidence as to such a belief nor, given the nature of the unauthorised photographs, the manner of their obtaining and that the Hello! Defendants well knew that authorised photographs were shortly to be published by OK!, do I see any room for any conclusion that publication could reasonably be so regarded. That the public would be

interested is not to be confused with there being a public interest.

"237. . . . As for paragraph 6 [of Schedule 2 to the Act], it provides:-

"The processing is necessary for the purposes of legitimate interests pursued by the data controller . . . except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

"238. The Hello! Defendants did, in my view, have a relevant legitimate interest – the publication of their magazine to include coverage of the Douglas wedding – but paragraph 6 denies legitimacy to the processing to that end if it is unwarranted by reason of prejudice to the rights and legitimate interests of the data subjects. The provision is not, it seems, one that requires some general balance between freedom of expression and rights to privacy or confidence; where there is a real public interest in relation to the material in issue then in the case of the Press such a general approach will have been considered under section 32. Here (in the events which I have held occurred) the question is more simply whether the publication is unwarranted by reason of the prejudice to Mr and Mrs Douglas' legal rights. Paragraph 6 does not provide, as it so easily could have done, how serious has to be the prejudice before the processing becomes unwarranted and in point of language any prejudice beyond the trivial would seem to suffice. . . ."

Case commentary

Following the Court of Appeal in Campbell, this judgment reiterates the approach to interpretation of some of the more 'routine' aspects of the DPA 98. The particular approach of the learned judge to interpretation of paragraph 6(1) of Schedule 2 to the Act is welcomed by the Commissioner. It properly reflects the weight that the Directive attributes (see Recital 30 and Article 7) to prejudice to the rights and freedoms or legitimate interests of individual data subjects. Any such prejudice is likely to override the legitimate interests of a data controller. As such it would be wrong to approach paragraph 6(1) as a balancing test unless it was recognised that such prejudice to a data subject would weigh heavily in that balance.

Financial matters

Financial Position to 31 March 2003

Data Protection Functions

The notification fee is set by the Lord Chancellor, and in making any fee regulations, the Lord Chancellor shall have regard to the desirability of securing that the fees payable to the Commissioner are sufficient to offset the expenses incurred by the Commissioner and the Information Tribunal in discharging their data protection (DP) functions and any data protection expenses of the Lord Chancellor in respect of the Commissioner or the Tribunal.

The table below excludes expenditure made on freedom of information functions, and is the Commissioner's calculation of the current position regarding recovery of costs through the notification fee.

Year ended 31-Mar	Office DP Expenditure In Cash Terms	Other DP Expenditure In Cash Terms (note 1)	DP Receipts In Cash Terms (note 2)	Cumulative Financial Position In Cash Terms	Cumulative Financial Position In Accruals Terms (note 3)	Accrued DP Fees (note 4)
£'000	£'000	£'000	£'000	£'000	£'000	£'000
1985	308	31	-	(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)	(9,191)	1,503
1993	3,723	78	7,842	(389)	(9,469)	5,903
1994	3,449	83	4,494	573	(7,913)	5,519
1995	3,798	69	3,420	126	(6,417)	3,673
1996	3,975	64	7,072	3,159	(5,526)	5,752
1997	4,025	65	5,173	4,242	(4,471)	5,697
1998	3,660	79	4,913	5,416	(2,527)	4,864
1999	4,190	82	7,586	8,730	(830)	6,538
2000	4,704	94	5,617	9,549	339	9,131
2001	4,970	90	2,076	6,565	1,431	5,047
2002	6,356	105	5,217	5,321	2,596	3,950
2003	9,501	112	8,398	4,106	5,471	4,605
Totals to 31 March 2003	71,581	1,447	77,134	4,106	5,471	4,605

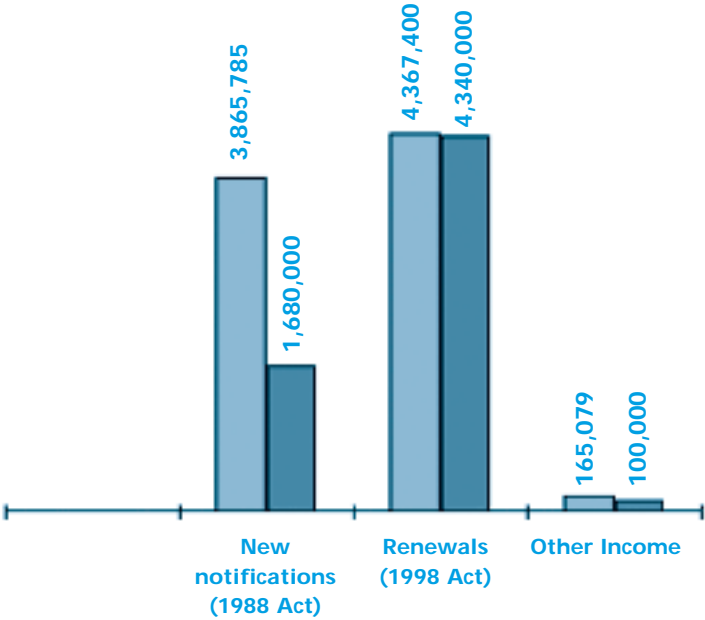
Notes:

1. 'Other expenditure' includes that incurred in respect of the Information Commissioner, the Information Tribunal and related Home Office/Lord Chancellor's Department costs.
2. 'Receipts' include notification fees and other receipts such as interest on unallocated grant-in-aid in hand.
3. From 1992 onwards, the cumulative position under accruals accounting principles is given, adopting a 'full cost' approach. From 1985 these figures incorporate notional costs and are also subject to the Treasury 'GDP deflator'.
4. Under the accruals method of accounting, fees received have been spread over the three year registration period and notifications over one year, thus providing an 'accrued fees' figure to be carried forward to future years.

Analysis of actual and forecast income 2002/2003

(in cash terms)

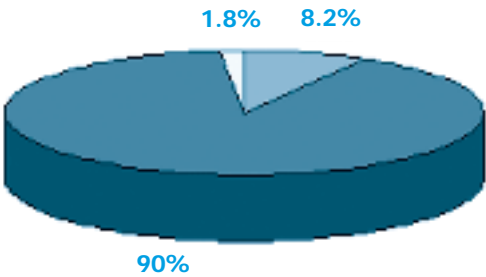
Actual		£
46.0%	New notifications (1988 Act)	3,865,785
52.0%	Renewals (1998 Act)	4,367,400
2.0%	Other Income	165,079
100.0%		8,398,264
Forecast		£
27.5%	New notifications (1988 Act)	1,680,000
70.9%	Renewals (1998 Act)	4,340,000
1.6%	Other Income	100,000
100.0%		6,120,000



Analysis of forecast income 2002/2003

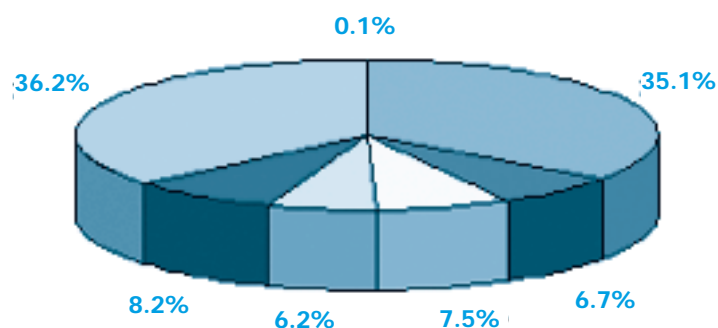
(in cash terms)

		£
8.2%	New notifications (1988 Act)	700,000
90.0%	Renewals (1998 Act)	7,650,000
1.8%	Other income	150,000
100.0%		8,500,000

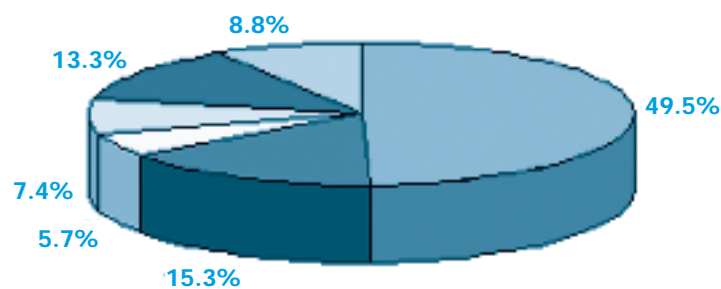


How the grant was spent 2002/2003*(in cash terms)*

35.1%	Staff and staff related costs	4,436,871
6.7%	IT Support	844,932
7.5%	Other running costs	949,694
6.2%	Accommodation	781,246
8.2%	Education and awareness	1,039,945
36.2%	Capital expenditure	4,573,041
0.1%	Grant in aid carried forward	980
<u>100.0%</u>	<u>Total</u>	<u>12,626,709</u>

**Our spending plans for 2003/2004***(in cash terms)*

		£
49.5%	Staff costs	5,823,734
15.3%	IT Support	1,795,000
5.7%	Other running costs	671,000
7.4%	Accommodation	867,000
13.3%	Education and awareness	1,561,000
8.8%	Capital Expenditure	1,028,000
<u>100.0%</u>	<u>Total</u>	<u>11,745,734</u>



Output Measures and Performance Indicators

Financial Years 2001/2002 to 2005/2006

Notification

	Actuals	Ests / Targets	Actuals	Estimates and Targets		
	2001 / 2002	2002 / 2003	2002 / 2003	2003/2004	2004/2005	2005/2006
Number of weighted transactions processed	334,567	361,223	505,754	415,427	354,542	365,288
Number of weighted transactions processed per officer day	79.53	82.61	88.02	127.14	118.36	121.95

There are three notification 'products' - new applications, and transformations (from 1984 Act renewals), renewals and changes. Each product is weighted in accordance with its processing time to year-on-year comparisons of performance to be made, reflecting the differing workloads encountered. The 'processed per officer day' figures incorporate different levels of staff from year to year and encompass increased productivity targets, and are calculated from the 'weighted' figures.

Transformations cease during FY 2003 / 04.

The target for processing weighted transactions has been revised to reflect the improved systems of handling the notification products.

Assessments and Complaints

	Actuals	Ests / Targets	Actuals	Estimates and Targets		
	2001 / 2002	2002 / 2003	2002 / 2003	2003/2004	2004/2005	2005/2006
Total requests for Assessment received	12,479	13,500	12,001	12,866	13,500	14,500
Handled as Enquiries	5,947	6,548	5,677	6,086	6,386	6,859
No Assessment made	754	945	1,317	1,411	1,481	1,591
Sub-total	6,701	7,493	6,994	7,497	7,867	8,450
Assessments completed*	5,929	6,480	4,564	4,893	5,134	5,514
Complaints from the 1984 Act closed	112	120	244	57	0	0
Sub-total	6,041	6,600	4,808	4,950	5,134	5,514
Number closed per Officer day	1.13	1.13	0.72	0.77	0.80	0.86

*Assessments completed comprise 'Telecom Regulations, Consumer Credit Act cases and request for assessment completed.'

Currently there are still complaints being investigated (made under the provisions of the 1984 Act).

Requests for assessment made under the 1998 Act are processed differently from complaints.

From 2000 / 2001 the number closed per officer day figure encompasses complaints closed and assessments completed.

Contact with our customers

	Actuals	Estimates/Targets	Actuals	Estimates and Targets		
	2001 / 2002	2002 / 2003	2002 / 2003	2003/2004	2004/2005	2005/2006
Telephone Enquiries received by the Information Line	56,982	57,000	59,486	75,000	75,000	77,500
Calls received per line hour	9.36	9.36	9.21	7.36	7.36	6.34

Contact is to all areas of the Office. Notification has its own dedicated enquiry line and media enquiries are dealt with by Marketing. Sector teams receive calls from data controllers and individuals with whom they have had previous contact. The Information Line handles all general calls, from controllers and individuals, and calls that have been transferred by the switchboard, currently these represent approximately 21% of the total calls received by the Office. Telephone enquiry figures represent the calls received by the Information Line.

‘Line hours’ are the hours spent by staff dealing with enquiries on the Information Line. The target figures for the ‘calls received per line hour’ are based on efficiency improvements being achieved year on year. For future years the intention is to have more lines open to improve the enquiry service given to customers.

Data Protection – Public Awareness

	Actuals	Estimates/Targets	Actuals*	Estimates and Targets		
	2001 / 2002	2002 / 2003	2002 / 2003	2003/2004	2004/2005	2005/2006
% large data controllers aware of subjects' rights	83	85.0	95.0	96.0	96.0	97.0
% small data controllers aware of subjects' rights	56	60.0	90.0	92.0	92.0	94.0
% data subjects aware of own rights	42.0	42.0	74.0	78.0	80.0	82.0

Freedom of Information – Public Awareness

	Actuals	Estimates/Targets	Actuals*	Estimates and Targets		
	2001 / 2002	2002 / 2003	2002 / 2003	2003/2004	2004/2005	2005/2006
Amongst the public (percentage)	12.0	15.0	49.0	50.0	60.0	65.0
Within public authorities (percentage)	23.0	25.0	53.0	60.0	65.0	65.0

Notes:

* Figures for 2003 show prompted awareness. Previous figures have shown un-prompted awareness.

Public Awareness and Awareness of Rights

The figures are based on annual tracking research conducted in the spring of each year.

Anyone requiring more detailed statistics and information is welcome to apply to the Office.

An increasing number of enquiries are now received by e-mail, letters also continue to be received.

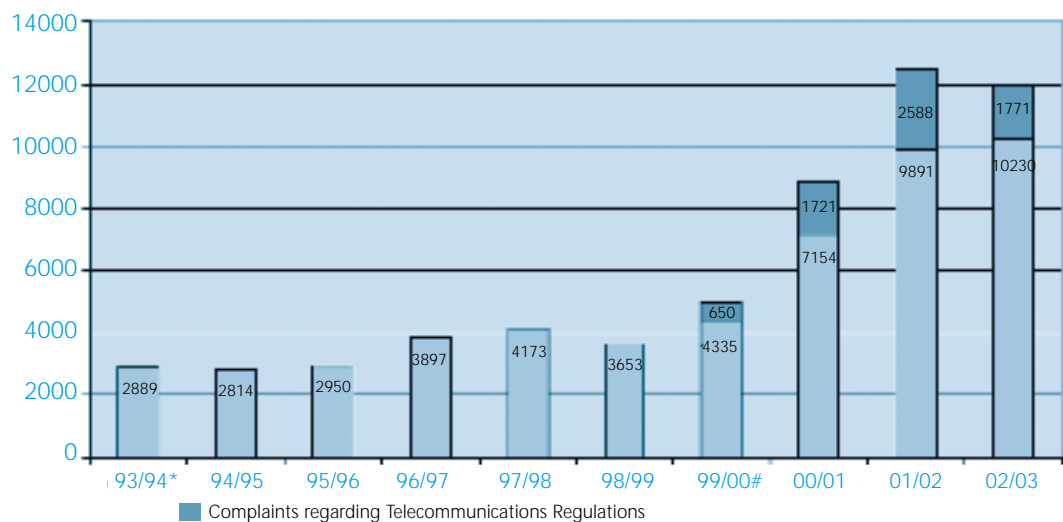
Our Annual Caseload

Requests for assessment

Section 42 of the Data Protection Act provides that persons who believe they are directly affected by any processing of personal data may request the Commissioner to make an assessment of whether the processing is likely or unlikely to have been carried out in compliance with the Act. In practice most requests for assessment are complaints from individuals who believe that their personal data have not been processed in compliance with the Act. In a considerable number of cases, though it is clear that the person making the request has concerns regarding the processing in question, we are not provided with sufficient information to enable us to make an assessment but are able to provide authoritative advice. Such cases, where we provide written advice, are counted as enquiries. These are to be distinguished from requests from data controllers for advice regarding their own compliance. Alleged breaches of the Telecommunications Regulations are not technically requests for assessment but are included in our caseload figures.

The total of requests for assessment, and those 'complaints' where an assessment is not made but which are recorded as enquiries, may be broadly compared with the annual totals of complaints under the Data Protection Act 1984. There was an annual total of some 12,001 requests for assessment and enquiries received during the year (including 1,771 complaints of breaches of the Telecommunications Regulations).

Complaints/requests for assessment received 1993 to 2003



Complaints/requests for assessment received 1993 to 2003

* Figures before 1994/95 refer to the financial year commencing 1 June to 31 May. Since 1994/95 figures refer to the financial year commencing 1 April to 31 March.

This figure for the financial year 1999/2000 is based on the number of complaints received for the eleven months to 29 February 2000, adjusted to provide a twelve month estimate.

Requests were received about:

	Percentage
Cases completed by the team dedicated to consumer credit work	20%
Cases relating to work falling under Telecommunications (Data Protection and Privacy) Regulations 1999	15%
Other	65%

A proportion of requests from individuals require our compliance teams to ask for further information from the individual and from the organisation concerned. This, along with the varying complexity of the cases themselves, results in the time taken to undertake these assessments varying considerably.

Of the number of cases closed:

	Percentage
Open for more than 12 months	1%
Open for 6-12 months	4%
Open for 3-6 months	6%
Open for 0-3 months	89%

Recorded outcomes

	Percentage of closed figure
Advice given (includes telecoms)	58.20%
Request for assessment declined	7.10%
Threshold criteria not met	6.50%
Unverified assessment – compliance unlikely	9.20%
Verified assessment – compliance unlikely	7.10%
Unverified assessment – compliance likely	7.60%
Verified assessment – compliance likely	4.30%

[1] There are other outcomes which relate to specific telecom regulations, consumer credit and non-notification project outcomes. The outcome percentages have been calculated to show as 100% of only those outcome categories listed above.

*Figures have been rounded to nearest percentage

*The threshold criteria are:

- whether the request is made by or on behalf of a person who is, or who believes themselves to be directly affected by the processing in question;
- whether we are satisfied as to the identity of the person making the request;
- whether we can identify the processing in question;
- whether the processing is of personal data.

Assessments outstanding

As of 31 March 2003 there were 1,788 cases received but not completed.

Complaints outstanding

Over 57 complaints made under the Data Protection Act 1984 remain under consideration. Some of these are with our investigations and legal teams for follow up action. During the year we closed 244 of such cases.

Investigations

The Investigations Department is responsible for the field investigation of alleged criminal breaches of the Data Protection Act, comprising:-

- interviewing witnesses and obtaining witness statements,
- obtaining and executing search warrants,
- conducting tape-recorded interviews with suspected offenders, under caution,
- reviewing evidence and preparing prosecution files and
- forwarding files to the Legal Department with recommendations of prosecution, caution or no further action.

Investigation and prosecution statistics	Year 98/99	Year 99/00	Year 00/01	Year 01/02	Year 02/03
Visits to business premises	700	388	480	448	573
Visits to dwellings	319	199	235	411	332
Witness statements obtained	433	346	355	375	513
Interviews under caution conducted	216	098	144	058	076
Demands for access to premises	002	002	-	001	003
Search warrants obtained	010	011	009	003	005
Regional Investigators	006	005	007	005	005
HQ Investigators	004	002.5	002	002	004

During this Commissioner's year, investigators made 905 visits to premises and were responsible for the recording of 513 witness statements and conducting 76 interviews under caution. To assist in their investigations, five search warrants were obtained.

The Investigations Department is also the host of the 'Non-Notification Project' which commenced in April 2002. During its first year, the team has looked at 2899 potential data controllers and encouraged 680 of them to notify.

Legal Proceedings

Prosecutions	2000/01	2001/02	2002/03
Number of offences brought to Court	23	66	91
Number of offences withdrawn/or on which no evidence offered		16	11
Number of offences acquitted after trial		8	-
Number of offences to lie on file		9	-
Number of offences resulting in a finding of guilt	21	33	80
Cautions administered	12	13	11*
Offences taken into consideration			601

* See further breakdown

Convictions 1984 Act	2000/01	2001/02	2002/03
Unregistered data users	13	2	2
Cases of unlawfully procuring information	4	18	19
Cases of selling unlawfully procured information	-	-	3
Cases of data users using data for unregistered purposes	1	12	1
Employee for using data for unregistered purpose	-	-	-
Data user for disclosing data	3	-	-
Employee for disclosing data	-	1	-

Convictions 1998 Act	2000/01	2001/02	2002/03
Obtaining personal data			33
Disclosing personal data			1
Selling personal data			20
Non notification			1

Cautions 1984 and 1998 Acts	2000/01	2001/02	2002/03
1984 non registration			3
1998 non notification			5
1998 obtaining personal data			2
1998 disclosing personal data			1

Enforcements

1 April 2002 to 31 March 2003

Enforcement	2000/2001	2001/2002	2002/2003
Preliminary Enforcement Notices	5	3	2
Preliminary Enforcement Notices leading to Enforcement Notices	1	2	1
Enforcement Notices	4	4	4
Preliminary Information Notices	-	-	3
Preliminary Information Notices leading to Information Notices	-	-	1
Information Notices	-	-	1

Notes

1 Enforcement Notice served on 21st Century Faxes Limited, Info 4U Limited, Right 2 Vote Limited, Hyperos Systems Limited, Launchasset Limited, Green Freephone Pages Limited, The Lord's Witnesses and two directors of those Companies

1 Enforcement Notice served on Petworth Publishing Limited and one director

91 cases were put before the criminal courts and 80 of them resulted in conviction. Of these 80 convictions secured in the Courts this year, only 2 resulted from the offence of being an unregistered data user (section 5(1) of the Data Protection Act 1984 (the "1984 Act")). This reflects the Commissioner's policy of reducing the priority in pursuing those unregistered data users who would not need to notify under the Data Protection Act 1998 (the "1998 Act") during the transitional period.

The majority of the prosecutions secured in the courts this year were offences under the 1998 Act. Many of the prosecutions under the 1984 Act are now concluded.

The Commissioner continues to investigate and prosecute cases which are complex evidentially. The cases involve time consuming investigation and preparation including the gathering of substantial amounts of evidence.

Pleas were accepted to a limited number of offences in one case, in the public interest, to preclude the need for a trial where it was considered by the Commissioner that sentence would not be affected adversely by the acceptance of such pleas. In that case the remaining offences were withdrawn by the Commissioner as appropriate.

The figure of 11 cautions this year demonstrates the Commissioner's continuing policy to administer cautions as an alternative to prosecution, where appropriate.

Prosecutions 1 April 2002 – 31 March 2003

Defendant	Offence	Court	Date of Hearing	Plea	Result	Sentence	Costs
Kevin Peter O'Connor	55(1)Obt	Sunderland Magistrates	10/05/02	Not Guilty	Convicted	£250	£500
	55(1)Dis			Not Guilty	Convicted	£250	
		Durham Crown	05/09/02	Appeal against conviction & sentence	Appeal withdrawn		
Dixons Motor Holdings Ltd	55(1) Obt	Grimsby Crown	30/07/02	Guilty	Convicted	£1000	No order for costs
Alistair Fraser t/a Solent Credit Control	55(1)Attempt Obt	South East Hampshire Magistrates	21/08/02	Guilty	Convicted	£100	£1000
	55(1)Attempt Obt			Guilty	Convicted	£100	
	55(1)Attempt Obt			Guilty	Convicted	£100	
	55(1) Obt			Guilty	Convicted	£100	
	55(1) Obt			Guilty	Convicted	£100	
	55(1) Obt			Guilty	Convicted	£100	
	55(4) Selling			Guilty	Convicted	£100	
	55(4) Selling			Guilty	Convicted	£100	
	55(4) Selling			Guilty	Convicted	£100	
	5(1) 1984			Guilty	Convicted	£250	
	17(1)			Guilty	Convicted	£250	
	66 tics						
London Borough of Islington	5(2) 1984	Highbury Corner Magistrates	20/09/02	Guilty	Convicted	£3000	£2350
Naser Hafeez as manager of Arena Credit Services Ltd	5(6) 1984 attempt as manager	Enfield Magistrates	28/10/02	Guilty	Convicted	£150	£1600
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	
	5(6) 1984 attempt as manager			Guilty	Convicted	£150	

[illegible]

Prosecutions 1 April 2002 – 31 March 2003 (*continued*)

Defendant	Offence	Court	Date of Hearing	Plea	Result	Sentence	Costs
Karen Pritchard <i>continued</i>	55(4) selling 55(4) selling 55(4) selling 55(4) selling 55(4) selling 55(4) selling 55(4) selling 55(4) selling 55(4) selling 348 tics			Guilty Guilty Guilty Guilty Guilty Guilty Guilty Guilty Guilty	Convicted Convicted Convicted Convicted Convicted Convicted Convicted Convicted Convicted	£50 £50 £50 £50 £50 £50 £50 £50 £50	
Raphel Ricardo Codrington	5(6) 1984 5(6) 1984 55(1) obt 55(1) obt 55(1) obt 55(1) obt 55(1) obt 55(1) obt 55(1) obt 55(1) obt	Kingston Crown	21/11/02	Not Guilty Not Guilty Not Guilty Not Guilty Not Guilty Not Guilty Not Guilty Not Guilty Not Guilty Not Guilty	Convicted Convicted Convicted Convicted Convicted Convicted Convicted Convicted Convicted Convicted	£50 £50 £50 £50 £50 £50 £50 £50 £50 £50	£1500
Samantha England as director of Intersearch Ltd	5(1) 1984 5(6)attempt as director 1984 5(6) as director 1984 5(6)attempt as director 1984 5(7) as director1984 127 tics	Brecon Magistrates	14/02/03	Guilty Guilty Guilty Guilty Guilty	Convicted Convicted Convicted Convicted Convicted	£200 £100 £100 £100 £100	£300

Notes

55(1) Obt means obtaining personal data.

55(1) Dis means disclosing personal data.

Unless otherwise stated all offences are breaches of the 1998 Act

In addition to the above table:

- 4 offences under Section 5(6) of the 1984 Act against an individual were withdrawn.
- 1 offence under Section 5(1), 1 offence under 5(7) and 3 offences under 5(6) of the 1984 Act against a company were withdrawn when the company ceased trading.

Information Commissioner – Annual Report and Accounts 2003

Notification Department Statistics

The Data Protection Register	2001/2002	2002/2003
Total Register Entries	198,519 (31.03.02)	211,251 (31.03.03)
New Applications	99,637	110,451
Made under the Data Protection Act 1998		
Renewals		
Requests for renewal made under the 1998 Act	46,219	124,782
Requests for Amendment	25,834	35,625
Under the 1984 Act	16,483	14,392
Under the 1998 Act	9,351	21,233

Third Party Agency Work	2002/2003
Total Notifications incoming post in FY 2002 - 03	110,563
Third Party Agency Notifications	11,940 10.80%
During FY 2002 - 03:	
The Notification Help Desk / Call Centre recorded	120,486 calls
of which, calls relating to third party agencies were	32,029 26.58%
Work caused by third party agencies greatly affected backlogs, e.g.,	
At Stage 1 Processing, the total backlog at the end of FY 2002 - 03 (31.03.03) was	6,311
of which, the backlog relating to third party agencies were	5,822 92.25%

The above figures were recorded throughout the financial year.

The numbers of letters and queries that relate to agencies were only recorded from January 2003, so there are insufficient data to base comments upon.

The Information Line, also, only began recording calls that applied to agencies in January 2003, so there are also insufficient data to base comments upon.