

S
3001

PREM 19/2219

NEW FILE COVER

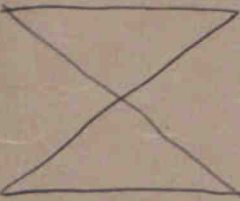
Confidential Filing

Data Protection

HOME AFFAIRS

PART 1

NOVEMBER 1980

Referred to	Date	Referred to	Date	Referred to	Date	Referred to	Date
29.6.84							
7.7.84							
13.10.86							
22.5.86							
30.9.87							
12.10.87							
20.9.87							
<p>PREM 19/2219</p>							
							
PART ENDS							

PART 1 ends:-

PMG TO SS/HOME 30.9.77

PART 2 begins:-

SS/DES TO PMG 12.10.77

TO BE RETAINED AS TOP ENCLOSURE

Cabinet / Cabinet Committee Documents

Reference	Date
H(80) 77	27.11.80
H(80) 79	28.11.80
H(80) 25 th Meeting, Minute 1	02.12.80
H(81) 8	05.02.81
H(81) 4 th Meeting, Minute 1	10.02.81
IT(82) 5	08.02.82
H(82) 6	16.02.82
H(82) 4 th Meeting, Minute 1	23.02.82
H(82) 33	29.06.82
H(82) 12 th Meeting, Minutes	07.07.82
CC(82) 48 th Conclusions, Minute 1 (extract)	11.11.82
H(82) 51	22.11.82
H(82) 52	24.11.82
H(82) 21 st Meeting, Minutes	29.11.82
L(82) 104	13.12.82
L(82) 21 st Meeting, Minutes	21.12.82
L(83) 65	15.06.83

The documents listed above, which were enclosed on this file, have been removed and destroyed. Such documents are the responsibility of the Cabinet Office. When released they are available in the appropriate CAB (CABINET OFFICE) CLASSES

Signed Wayland

Date 29 October 2015

PREM Records Team

Published Papers

The following published paper(s) enclosed on this file have been removed and destroyed. Copies may be found elsewhere in The National Archives.

House of Commons Hansard, 30 January 1984,
Columns 30-110 "Data Protection Bill"

Signed Wayland Date 29 October 2015

PREM Records Team



cc B4

PD3 1/10

Treasury Chambers, Parliament Street, SW1P 3AG

The Rt Hon Douglas Hurd CBE MP
Secretary of State
Home Office
50 Queen Anne's Gate
LONDON SW1H 9AT

30 September 1987

Dear Douglas,

DATA PROTECTION

I recently met Eric Howe, the Data Protection Registrar, at his request. The focus for the meeting was the passage in his last annual report (extract attached) about the proposed Government Data Network, for which I am the Chairman of the Steering Committee. I explained my role in this multi-Departmental project, and made clear to him that it has not yet been finally decided whether to proceed.

However, the meeting broadened out to discuss the issues raised in the fifth paragraph of the extract, which are relevant to any personal data held by Government Departments in automated form, and not simply to those applications which are currently planned to be put onto the GDN. I made it clear to Mr Howe that these issues went beyond my own responsibilities, and were a matter for individual Departments - within the constraints laid down by statute and any assurances which Ministers have given to Parliament. Mr Howe accepted this, but indicated that he would wish to discuss the issues with officials in individual Departments. As you will see from the extract, he is seeking greater visibility for the rules which govern data interchange and the way in which they are managed. He also has it in mind to establish a code of practice.

He may therefore be approaching your officials in due course. How you would wish your officials to handle such an approach is of course a matter for you. But my belief is that the Government's record on data interchange is generally a good one, and that we have much to gain by proving this to the independent Data Protection Registrar. If you agree, then you may wish to ask your officials to respond as constructively as possible to

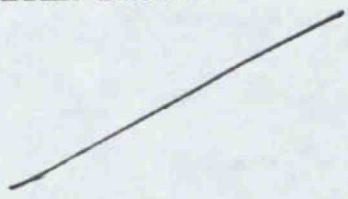
any approach from Mr Howe, and to keep CCTA in touch with any discussions.

I am copying this letter to Ministers in charge of Departments.

Lumsden

Pm

PETER BROOKE



~~Data Protection Act can be taken fully into account if and when changes are made to the law governing Share Registers.~~

(iv) The Proposed Government Data Network

There has also been public debate about the proposed Government Data Network. This network has the objective of reducing costs and providing more effective administration for four major Government departments—Health and Social Security, Customs and Excise, Inland Revenue, and the Home Office.

Advancing communications technology can facilitate the cross-connection of different collections of information. Concern has been expressed that this could lead to the creation of what are effectively massive and comprehensive databases of information, possibly concerning the whole population.

The Government Data Network is important therefore, not simply in its own right, but because it potentially allows the wider use of information across Government departments. Whether this potential should be created is a matter for Government and Parliament. In reaching a decision, the issues of data protection are important factors as well as questions of efficiency and cost.

Obviously, it will be very important for the network to maintain the integrity of the information passing across it by preventing it from being lost, destroyed, stolen, tampered with or corrupted. But it is in the use of the network that the key issues lie. Even without the network, disclosures of personal data by Government departments can raise sensitive issues. With the network, these issues come into sharper focus. I am sure it would be helpful if the public could clearly see how these issues are resolved. The Data Protection Register can be of some limited help here. An analysis of the entries for the various Government departments concerned can give a broad indication of the general pattern of disclosures, but it cannot give a precise picture.

I have been pleased by statements that Government departments impose their own strict rules on disclosures of personal data from one to another. I believe it would be valuable if these rules were published. This would help to ensure an informed public debate on data protection and privacy issues. It would also be helpful if the ways in which the rules were managed were made known. Are there exceptions to them? At what level are decisions made on the rules and the application of them? Are there disciplinary proceedings for breaches of the rules? What review and monitoring procedure is in operation? Are reports made available on the way in which the rules work in practice?

I was approached in September 1986 by the Director of the Central Computing and Telecommunications Agency (CCTA) to see what assistance and advice I might provide in connection with proposals for protecting the security of personal data passing across the proposed network. I welcome this approach and the concern it shows for an important Data Protection Principle and have offered to comment on proposals at a general level. This is similar to the assistance given to trade associations which are developing data protection codes of practice. I do not have the resources to give deeper support. There is also the question as to how far I should devote significant resources, ultimately to be paid for by registration fees from Data Users generally, to the problems of one Data User, albeit those problems may be very significant.

(v) A possible "National Credit Reference Register"

~~Sensitive databases covering the mass of the population are not restricted to the public sector. They occur, for example, in connection with credit reference information. Proposals to develop collections of this type of information into what has been called a "national credit reference register" raise important issues. Whilst proposals do not seem to be fully defined as yet, I am concerned to ensure that the objectives and requirements of the Data Protection Act are taken fully into account.~~

~~With any large collection of sensitive personal information the Data Protection Principles should be applied with particular diligence and care. Is the~~

CONFIDENTIAL

file

GA



10 DOWNING STREET

From the Principal Private Secretary

SIR ROBERT ARMSTRONG

DATA PROTECTION ACT

I have shown the Prime Minister your minute of 21 May in which you ask her to sign a certificate required under the Data Protection Act relating to information held on the computer regarding reports on leak investigations. The Prime Minister has now signed the certificate which I herewith return.

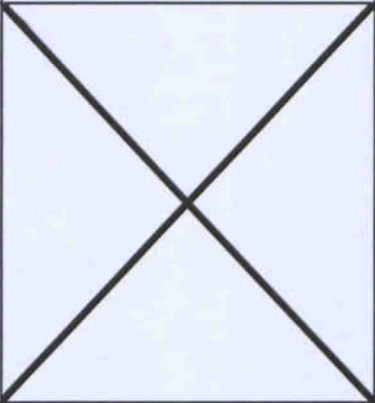
N.L. WICKS

22 May 1986

CONFIDENTIAL

GA

A The National Archives

DEPARTMENT/SERIES <i>PREM 19</i> PIECE/ITEM <i>2219</i> (one piece/item number)	Date and sign
Extract details: <i>Armstrong to Wicks dated 21 May 1986</i>	
CLOSED UNDER FOI EXEMPTION	
RETAINED UNDER SECTION 3(4) OF THE PUBLIC RECORDS ACT 1958	
TEMPORARILY RETAINED	<i>13/2/2016</i> <i>S. Gray</i>
MISSING AT TRANSFER	
NUMBER NOT USED	
MISSING (TNA USE ONLY)	
DOCUMENT PUT IN PLACE (TNA USE ONLY)	

file

DSG

MRS. COLE

cc Mr Wicks

DATA PROTECTION ACT

MPO have invited me to attend a meeting to discuss registration under the DPA. I have been invited as the No. 10 representative. The meeting is due to take place at 1030 on 24 January.

I wonder if this is not something which it would be more appropriate for you to take on. Let us have a word about this if you like. Gloria Ryan is the MPO contact: telephone 233 4415.

MEA

Mark Addison

13 January 1986

(DSG.43)



PRIVY COUNCIL OFFICE
WHITEHALL, LONDON SW1A 2AT

7 July 1984

Dear Grey.

Dr Biff

PERSONAL RECORDS: TEN MINUTE RULE MOTION: TUESDAY 10 JULY

Thank you for your letter of ~~29~~ June about Chris Smith's motion next Tuesday to introduce an Access to Personal Files Bill.

I note that you draw a clear distinction between individuals' access to information about them and the general statutory right of access to official information which is proposed in David Steel's Bill. Nevertheless, I agree that any legislation on this difficult issue must be preceded by thorough preparation and consultation; and that it would not be right for the Government to allow a Bill to make progress until it is satisfied that change is desirable and feasible. I agree therefore that this Bill should be blocked at Second Reading, and that Ministers should abstain if the House divides on Tuesday.

John Biffen

JOHN BIFFEN

Rt Hon the Earl of Gowrie
Minister for the Arts
Cabinet Office

Copies of this letter go to:

Prime Minister

Members of Legislation Committee

Secretary of State for Foreign and Commonwealth Affairs

Secretary of State for the Home Department

Chancellor of the Exchequer

Secretary of State for Education and Science

Secretary of State for Energy

Secretary of State for Defence

Secretary of State for the Environment

Secretary of State for Social Services

Secretary of State for Employment

Secretary of State for Trade and Industry

Secretary of State for Transport

Minister for Agriculture, Fisheries and Foods

Chief Secretary, Treasury

Sir Robert Armstrong

Minister for Overseas Department, Foreign and Commonwealth Office

First Parliamentary Counsel

Home Affairs : Data Protection Nov 80.



JUL 1984



CABINET OFFICE

From the Minister of State

Lord Gowrie

MANAGEMENT AND PERSONNEL OFFICE

Great George Street

London SW1P 3AL

Telephone 01-233 8610

The Rt Hon John Biffen MP
 Lord Privy Seal
 Whitehall
 London SW1

29 June 1984

Dear Sir,

PERSONAL RECORDS: TEN MINUTE RULE MOTION: TUESDAY 10 JULY

On Tuesday 10 July, Chris Smith will seek to bring in a Bill to give individuals a right of access to certain kinds of personal data about themselves. The Motion reads,

ACCESS TO PERSONAL FILES: That leave be given to bring in a Bill to provide access for private individuals to certain classes of information maintained by certain authorities and institutions.

The Bill is a further move by the Campaign for Freedom of Information. David Steel's Freedom of Information Bill is down for Second Reading on the previous Friday, 6 July, when we have agreed that it should be blocked (your letter to me of 5 March). Simon Hughes' Local Government (Access to Information) Bill, the Campaign's third Bill, will, I understand, also be blocked at Second Reading on 6 July.

The Campaign have not made clear exactly what Chris Smith's Bill will cover. Their literature earlier this year suggested that the likely areas were

- a. education
- b. social services
- c. local authority housing, and
- d. medical records,

CONFIDENTIAL

but that the Bill might go wider and even into the private sector. Parliamentary Questions by Chris Smith in April tended to confirm that the main areas would be as above, with the possible addition of social security benefits, tax assessments under appeal, criminal records, and visiting allowances for prisoners' families.

The David Steel Bill (though as I write it has still not been published) is unacceptable in principle; there are overriding constitutional objections to a statutory right of access to official information in general. But the same objections do not necessarily apply to individuals' access to their own records. The Data Protection Bill will bring about a major advance in this direction. It does not apply to manual records, but the arguments for restricting it to computerised data are ones of practicality rather than of principle; moreover, we have always recognised that it would be beneficial if the data protection principles (including access by the "data subject") that will be enforceable in respect of computerised data came to be applied to manually-held information also.

We would not want therefore to appear unsympathetic to the Bill's aims. It will in fact be helpful to us in resisting general freedom of information legislation (a Ballot Bill next session is extremely likely) if we can separate in the public mind access to personal records from access to information generally.

Nevertheless I think we are justified in rejecting this Bill. Preliminary work by my officials, in consultation with other departments, as indicated that the field is enormous and enormously complex. It is doubtful whether the Bill's authors have focused adequately on the problems, and inconceivable that they have undertaken the consultations that would be necessary if legislation on these lines were to have a chance of working. If we were criticised, I think we could simply point out that the Government could not give a fair wind to a Bill of this importance when it had had no time to consider the Bill properly or undertake the necessary consultations.

As to tactics, I suggest we should treat this Bill exactly like the David Steel Bill, ie not oppose the motion (and abstain if there is a Division) but ensure that it is blocked at Second Reading.

CONFIDENTIAL

I am sending copies of this letter to the Prime Minister, members of Legislation Committee, other Ministers in charge of Departments, Sir Robert Armstrong and First Parliamentary Counsel.

*Yours,
L. J. G.*

LORD GOWRIE

CONFIDENTIAL

010

TF

CONFIDENTIAL

Ref. No: HA(84)1

Date: 27.1.84

Data Protection Bill
2nd Reading
House of Commons
30th January 1984

Dr
31/1

Conservative Research Department,
32 Smith Square,
London SW1
Tel. 222 9000

Enquiries on this brief to:
Nigel Clarke

(1) Introduction to the Bill

The issue of statutory protection for personal information that is handled automatically was first assessed in the Report of the Younger Committee in 1972, set up by the Conservative Government in 1970 to examine the whole issue. It established a series of principles to apply to the handling of information.

The Council of Europe analysed the issues at length throughout the following decade, and produced in 1981 the European Convention for "the Protection of Individuals with regard to Automatic Processing of Personal Data". This was signed by the UK in May 1981; consequently it became necessary to introduce legislation so that the Convention could be ratified.

The Bill was drafted in the light of the Report of the Lindop Committee of 1978, which had been set up by the Labour Government in 1976 to examine the issues and make proposals for possible legislation. This Report was an extensive analysis of the problems of operating a satisfactory scheme of privacy safeguards, and contained a wide review of data protection matters. It proposed the establishing of legislation based upon the principles outlined by the Younger Committee, but also contained two sections which the Government could not accept.

Firstly, it proposed a multi-member Data Protection Authority to enforce the legislation. The Government rejected this in favour of an individual Registrar, independent of Government. Lord Whitelaw, then Home Secretary, argued:

"We see this as by far and away the most economical use of resources. Since the scheme will be funded by the data users themselves, this is of particular importance to them. We believe that an individual registrar will be able to act more rapidly, authoritatively and consistently in this complex and infinitely varied field than could a committee" (Hansard, 11th April 1983, Col. 557).

Secondly, the Report recommended codes of practice which would have created a host of new offences in criminal law. The Government did not consider that it was constitutionally right to confer responsibility for drafting a whole sector of criminal law on an independent authority, who would not have the competence to undertake a task that is properly one for Government and Parliament. Mr Timothy Raison, then Minister of State at the Home Department, summed up this view:

"In our approach ... we concentrated on putting the responsibilities where we believe they belong ... Our concern will be to establish a sound basic framework capable of being built on and expanded progressively with more detailed provisions as we gain experience." (Speech to BMA Conference on Data Protection, 15th September 1981).

The Bill will enable Data Protection arrangements in this country to be consistent with standards adopted in other European countries. It will ensure an atmosphere in which there is the highest possible degree of confidence that the individual citizens are not being put at risk by the spread of new technology.

The original Data Protection Bill fell at the announcement of the General Election. The Bill as reintroduced contains a number of changes, designed firstly to simplify the provisions as they relate to companies, and secondly to provide additional safeguards governing the exercise of the Registrar's powers of entry to the premises of data users. Mr David Waddington, Minister of State at the Home Office, summed up the purposes of these changes:

"These changes will make the Bill simpler to operate and, by easing the Registrar's workload, will enable him to devote more of his resources to the general oversight of data protection" (Home Office Press Release, 24th June 1983).

(2) The Bill's Proposals

Part I of the Bill establishes an independent Data Protection Registrar, appointed by the Crown, to enforce certain principles relating to personal data held on computers. These "Data Protection principles" are set out in clause 2 and Schedule 1, and provide that:

- (1) Data shall be obtained and processed fairly and lawfully;
- (2) It shall be held only for one or more specified and lawful purpose;
- (3) It shall be adequate, relevant and not excessive in relation to that purpose;
- (4) It shall be accurate and kept up to date;
- (5) It shall not be used or disclosed in any way incompatible with its purpose, nor held longer than is necessary for that purpose.

A data subject will be entitled at reasonable intervals without undue delay or expense, to access to data of which he is the subject, and, where appropriate, he may have such data corrected or erased. Unauthorized access to, or alteration, disclosure, or destruction of data, and accidental loss or destruction of data shall be subject to appropriate security measures. The provisions of the Bill will not apply to the use of word processors for the preparation of documents.

Part II of the Bill deals with the registration and supervision of data users and computer bureaux.

(1) The Register

Data users will be required to register the following information:

- (a) their name and address;
- (b) description of the data held by them and the purposes for which the data are to be held or used;
- (c) a description of the source of the data;
- (d) a description of any persons (other than the data subjects in question) to whom the data may be disclosed;
- (e) the names of any countries outside the UK to which the data may be transferred;
- (f) the name and address of an individual who will be responsible for dealing with requests from data subjects for access to the data.

Those who have applied to register, or to change their registered particulars, will in most cases be able to commence the activity in question immediately upon application to the Registrar.

(2) Duties and Powers of the Registrar

- (a) The Registrar will be required to maintain a register of specified details of users and the personal details they hold, which will be open to public scrutiny. It will be an offence to operate unregistered or in contravention of the registered details. Further to this, as Mr Timothy Raison, then Minister of State at the Home Office, stressed:

"The Registrar will have real teeth. He will have two key powers in relation to registered users. He will be able to serve notices requiring users to change their procedures to bring them into compliance with the general principles; and he will be able to strike a user off the register" (4th May 1982).

- (b) In circumstances where data is being transferred or will be eventually transferred to another country not bound by the European Convention if the use of the information is liable to breach the data protection principles, the Registrar may prohibit the transfer.
- (c) Schedule 4 of the Bill sets out the powers of entry and inspection available to the Registrar. A circuit judge may issue a warrant authorizing the Registrar, within 7 days of the issue, to access to premises if he is satisfied that there are reasonable grounds for suspecting an offence or breach of the data protection principles is being committed.

He may not issue a warrant unless the Registrar has given the occupier of the premises 7 days notice in writing demanding access at a reasonable hour; this access has then been refused unreasonably, and following this the Registrar has given notice of the application for a warrant so that the occupier has the opportunity to be heard by the judge.

(3) The Data Protection Tribunal

Appeals against the Registrar's decision will be heard by a specially constituted Data Protection Tribunal, with a legally qualified Chairman.

Mr Raison summed up the Bill's proposals for a graduated response from the Registrar in cases of breaches of the principles:

"In most cases, discussion, advice and persuasion will be all that is needed. A user who is ready to comply with the principles will face nothing more. But in those cases - I hope few - where the Registrar will need to exert more than that, he has the tools readily to hand" (4th May 1982, addressing the Parliamentary Information Technology Committee).

Part III of the Bill enables individuals to obtain details of personal data held about them, and to seek compensation from the courts for damage suffered by reason of inaccuracy or as a result of loss or unauthorised destruction or disclosure; or as a result of unauthorised access. Compensation will not be possible firstly in cases of inaccurate data which has been properly marked as 'received' information, and secondly in cases where the user has marked the data as being in dispute. Courts will have powers to ensure that the accuracy of such information is recorded as being in dispute.

Part IV of the Bill provides for exemptions from the Bill. These can be divided into two categories - total (those involving national security) and partial exemption.

(1) National Security

Personal data held or disclosed for national security purposes are to be exempt from the Bill. Clause 27 (4) provides that a certificate signed by a Minister of the Crown certifying this shall be conclusive evidence of the fact. A Minister of the Crown is defined as a member of the Cabinet, the Attorney General or Lord Advocate.

(2) Partial exemptions

There will be exemptions from certain provisions of the Bill where their application would be prejudicial to the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of any tax or duty. These exemptions have proved to be very contentious. Mr Raison stressed:

"The ability of our law enforcement agencies to prevent and detect crime must be protected. We will therefore provide, in accordance with Article 9 of the Council of Europe Convention, for data used for certain limited purposes to be exempt from the requirement to be registered. This will not mean that the police will be exempt. They will not be wholly exempt ... Much of the information held on the Police National Computer System will be fully within the scheme, fully accessible by the Registrar and fully accessible by data subjects.

Apart from these exemptions, all public users will be registered. But in some areas, again in accordance with the Convention, we believe it will be necessary to limit the right of data subjects to information about them. For example, we could not justify telling subjects about information which may be held on them during a murder enquiry " (London, 23rd June 1982).

(3) Companies

Data held by companies for paying staff or calculating their pay, and data held for accounting purposes will be excluded from registration.

(4) Health and Social Data

The Secretary of State may, by order, exempt from the subject access provisions data concerning the physical or mental health of the data subject, or data held for, or acquired during social work carried out in relation to the data subject.

(5) Judicial appointments and legal professional privilege

Exemptions from subject access provisions will also apply to data held by Government departments making judicial appointments, and data where there is a claim to legal professional privilege.

(6) Statistical and research data

This will be exempt from subject access provisions, provided that the results when made available are not in such a form that they identify the data subjects.

(7) Data held for domestic purposes

Data held by an individual and concerned only with the management of his personal, family or household affairs, are exempt from Parts II and III of the Bill.

(8) The exemption which previously applied to statistics concerned with immigration has been removed. Although this did not contravene the Council of Europe Convention (as suggested by some commentators) because it applied to employment protection, it was felt that such an exemption posed a risk to good race relations.

Part V of the Bill contains general provisions, including a requirement that the Registrar provide annual reports to Parliament. Additionally, Clause 36 deals with the application of the Bill to Government Departments and police forces. They will be subject to the same obligations under Parts II and III of the Bill as a private person, but will not be liable to prosecution. In some instances, however, it will be possible to take proceedings against individuals in the breach the Data Protection provisions.

The Secretary of State is empowered to appoint the day on which the registration process is to begin, and the Bill provides for a further 2 years transitional period before the Registrar's powers become fully operational.

(3) Labour's Position

The Labour Party are in favour of the Data Protection principles, but are in favour of a Data Protection Authority as opposed to a Registrar. On the issue of exemptions from provisions of the Bill, their position has been vague; Labour's Programme 1982 states:

"There would be some necessary exemptions; for instance, certain information relating to defence and foreign relations, to criminal investigations, etc., would need to be protected".

The Labour Party are also in favour of including all manually held data within the provisions of the Bill. Mr David Waddington summed up the Government's objection to this:

"To include manual data would add enormously to the work of the Registrar, and it is not the use of manual data but the computer's ability to retrieve, collate and transfer large amounts of data at high speed which poses the greatest potential threat to personal privacy and which has generated public concern" (Home Office Press Release, 24th June 1983).

The Labour Manifesto 1983 contained no detail and merely promised some form of legislation. The Labour Party abstained on 2nd Reading of the original Bill on 11th April 1983.

(4) Ratification of the Council of Europe Convention

It is proposed that the Convention will be ratified by the UK at the end of the two year transitional period when all the proposals of the Bill are fully operational.

NC/LC
27.1.84



HOME OFFICE
QUEEN ANNE'S GATE
LONDON SW1H 9AT

20 June 1983

Dr
21/6.

Jean de Waal,

DATA PROTECTION BILL

As you know this Bill is to be considered by the Legislation Committee tomorrow morning, Tuesday 21 June. We are hopeful that the Committee will approve immediate introduction of the Bill, in which case I should be grateful if you would arrange for its introduction in the name of Lord Elton in the House of Lords on Thursday, 23 June, with publication later that day if possible.

We are not having a Press Conference at the time of publication but there will be some press briefing and it would be helpful if 25 copies of the Bill addressed to Lord Elton could be available in the Printed Paper Office at the time of publication.

I am sending copies of this letter to Willie Rickett (Prime Minister's Office), Richard Watson (Cabinet Office), David Heyhoe (Lord President's Office), Murdo Maclean (Chief Whip's Office, Commons), David Beamish (Chief Whip's Office, Lords) and Brian Shillito.

Yours sincerely,

T C MORRIS
Parliamentary Clerk



The AA
cc CO

10 DOWNING STREET

From the Principal Private Secretary

24 February 1983

Dear Tony,

DATA PROTECTION BILL : HONOURS AND APPOINTMENTS

Thank you for your letter of 21 February enclosing a note about the problems of amending the Data Protection Bill to exempt from subject access records relating to honours and crown appointments. I have shown this to the Prime Minister, who has noted that in present circumstances it would be difficult to move an amendment to the Bill to provide these exemptions. It would be helpful, however, if you could keep this possibility under review if developments during the course of the passage of the Bill indicate that wider exemptions to subject access may be acceptable, since the present provisions will debar us indefinitely from introducing electronic methods for the access and retrieval of honours and appointments material in this office, at some cost in efficiency

I am copying this letter to Richard Hatfield (Cabinet Office).

Yours sincerely,

Robin Butler

A R Rawsthorne Esq.,
Home Office.

PRIME MINISTER

c.c. Mr. Catford
Mr. Flesher

DATA PROTECTION BILL: HONOURS AND APPOINTMENTS

Flag A

When you saw my minute of 8 February, you suggested that I should seek the Home Office's advice about the prospects of getting an amendment to the Data Protection Bill to exempt Crown appointments and honours from the requirement to give to individuals covered by such information access to it.

I have now discussed this with the Home Office, with the help of Robin Catford and Tim Flesher. The Home Office see difficulties in amending the Bill to provide exemptions for either honours or Crown appointments. Their reasons are set out in the attached note.

I understand the Home Office's difficulties about extending any further the exemption already given in respect of judicial appointments. The arguments used by the Lord Chancellor for exemption of information about judicial appointments apply to our honours and appointments, but they must also apply to information held in the personnel divisions of companies and other bodies up and down the land. Why should we be let off if they cannot be?

I am afraid that the trouble is the principle that a person can only be protected in respect of computer information held about him if he is given access to that information. In my view, that is a silly principle: why should people be given access to computer records about themselves but be denied access to manual records? The effect of it is that records which could have been stored efficiently using the sort of system we have put into our Correspondence Section will have to go on being kept manually, not just in this office but in hundreds of comparable offices.

It is maddening to think how that will inhibit the use of more efficient methods of storage and retrieval which computers give - and how much business will be lost to the computer industry as

/ a result.

a result. But I am afraid that this principle is at the heart of the Council of Europe Convention on Data Protection, and consequently of the Data Protection Bill.

So we have two options:-

- (i) to advise you to press the Home Secretary further for an exemption for either honours or Crown appointments, or both, despite the difficulties in the Home Office note;
- (ii) to accept the arguments of the Home Office' about the difficulty of extending the exemptions in this way and to deny ourselves the opportunity of bringing in the sort of system we have introduced in the Correspondence Section for the indefinite future.

With great reluctance, I am afraid that my conclusion is that we do not have a strong enough case to argue for (i) and that we therefore have to accept option (ii).

Do you agree?

F.R.B.

23 February 1983



HOME OFFICE
QUEEN ANNE'S GATE LONDON SW1H 9AT

21 February 1983

Dear Robin,

DATA PROTECTION BILL: HONOURS AND CROWN APPOINTMENTS

I understand that following your letter of 10 February to John Halliday, Ralph Shuffrey and David Chesterton discussed with you the problems about amending the Data Protection Bill to exempt from subject access records relating to honours and crown appointments. I now enclose a note setting out the difficulties as we see them.

I am afraid you will regard our response as very negative. But the Home Secretary feels that amendments to the Bill for this purpose would take us a long way down a very slippery slope. The exemption for judges took us over the top, but it has so far proved possible to hold the line there.

I am sending a copy of this letter to Richard Hatfield.

Yours,
Tony

A R RAWSTHORNE

E-1

DATA PROTECTION BILL: HONOURS AND CROWN APPOINTMENTS
General

The Bill already provides fairly extensive exemptions (particularly from subject access) for the public sector: national security, the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment and collection of any tax or duty, the control of immigration, and information relevant to the making of judicial appointments. By contrast the private sector gets very little exemption: data held by an individual and concerned only with the management of his personal, family or household affairs, and limited exemption for mailing lists.

2. Exemptions have to comply with the terms of the European Convention. The Convention specifically allows for them in the field of security, crime and "the monetary interests of the State" (which is taken to cover taxes and duties). The Convention also allows for exemptions in the interests of "protecting data subjects or the rights and freedoms of others", and it is on this basis that the immigration exemption is justified and, with some hesitation, that relating to judicial appointments.

3. When H Committee discussed on 29 November 1982 the Lord Chancellor's proposal for an exemption for judicial appointments the following was recorded in the minutes.

"In discussion of data about appointments, it was noted that the Lord Chancellor's misgivings were shared by the Lord Advocate. The problem, however, went much wider than judicial appointments; it also concerned, for example, recommendations for honours and the records of the Public Appointments Unit of the Manpower and Personnel Office, but those could not be exempted from the Bill. Industry had a problem over personnel records, and would keep at least part of such records on manual files. Such a procedure seemed necessary for Government as well."

4. There is considerable pressure to exempt "judgemental data" (i.e. expressions of opinion about individuals) from the provisions of the Bill, but it is clear that such a widespread exemption would be contrary to the practice followed in other

countries and contrary to the spirit of the Convention. While the application of information technology to honours, appointments and such matters may well speed up the handling of the work, it carries with it certain dangers. Opinions and assessments that can be reproduced instantaneously and therefore copied to a wide audience pose a greater threat to the individual to whom they relate than a manual file in a locked cupboard. This is one of the primary justifications for the Bill and the Convention.

Honours

5. Data relating to honours are mainly comprised of recommendations couched in highly complimentary terms. But it is not so much the contents of the data that would be threatened by subject access as the very fact that the data subject would be able to ascertain whether or not he had been recommended for an honour.

6. Such records are not confined to Government Departments. No doubt fairly elaborate lists of people considered suitable for honours are held in many large organisations in both the public and the private sectors. It would therefore not be easy to defend an amendment dealing with honours unless it was couched in pretty general terms.

7. It seems at least questionable whether it would be at all appropriate to incorporate into a statute a reference to the honours system.

Crown Appointments

8. If "Crown Appointments" covers any appointment by Royal Warrant, there is a great variety of them, ranging from Archbishops, Bishops and other Clergy, Lord Lieutenants and (for example) the Governors of Wellington School to some civil servants such as Her Majesty's Inspectors of Constabulary, Fire Inspectors and Prison Inspectors.

9. There are no principles on which one could distinguish such appointments (apart from the fact that they are made by the Queen) from others in the public sector: eg civil servants generally and Chairmen and Members of the boards of nationalised industries.

10. Again, one can scarcely draw the line at the public sector. The "head hunting" firms who help in the selection of board members and senior executives of companies in the private sector would have a strong interest in exempting their records. The spokesmen for the CBI in Parliament would not be slow to draw attention to this.

Conclusion

11. To sum up: personal data held for the purpose of making recommendations for honours or for appointments by the Crown are in principle very difficult to distinguish from data held for the purpose of making other important appointments or awards. The problems that result from subject access, for both the system and the flow of information from referees, are very similar and are to be found throughout the private as well as the public sector: amendments relating to honours or Crown appointments would raise the whole question of "judgemental" data (e.g. references); would be difficult, if not impossible, to confine to data held by Government; and would put us seriously out of step with other European countries.

cc Mr. Butler
Mr. Catford

NOTE FOR THE RECORD

We met Mr. Shuffrey and Mr. Chesterton of the Home Office today to discuss the Data Protection Bill in relation to our honours and appointments records. We argued that an exemption for honours and crown appointments was necessary to preserve the integrity of the systems of nomination for honours and appointments. Without an exemption we would be obliged to maintain on manual records information which could quite easily be computerised. Mr. Shuffrey and Mr. Chesterton made a number of points and I record the main ones below:

- (a) The range of crown appointments is extremely wide. It included for example fire inspectors as well as bishops and it would be difficult to maintain the case for their exemption from the provisions of the Bill.
- (b) The main purpose of the Bill was to enable this country to ratify the European Convention. Too wide an exemption would make us out-of-step with European practice.
- (c) If there was an exemption for honours and appointments the questions would arise of how far it should extend; should it extend for example to records held in the private sector as well as to Government departments?
- (d) The principal problem of presenting the Bill was the extent to which exemptions were already given for the public sector as opposed to the private sector. Any further exemptions would exacerbate the problem.

BF
It was agreed that the Home Office would re-examine the case for exemptions for honours and/or crown appointments and should provide a note before amendments had to be tabled for the report stage of the Bill (3 March) for the Prime Minister's consideration.

TF.

Tim Flesher

17 February 1983



10 DOWNING STREET

File AH

CCS. CO

Joan Porter

Daphne Edmunds

From the Principal Private Secretary

10 February 1983

RESTRICTED

Dear John,

DATA PROTECTION BILL

Tim Flesher wrote to Lesley Pallett on 8 December about the implications for No 10 of the Data Protection Bill. In her reply of 17 December she said that it would be difficult to exempt the kind of material held here from the provisions of the Bill.

XII I have now had a chance to discuss this with the Prime Minister and I fear that I must seek your advice once again. As you know, the only material currently held on computer at No 10 is that connected with our correspondence system. This system holds only such information as the names and addresses of the Prime Minister's correspondents and microfilmed records of their letters. We see no difficulty in giving the subjects of such data access to it, as required by the Bill.

We could not, however, contemplate giving similar access to the subjects of the records which we hold on honours and Crown appointments. In these circumstances, unless an exemption were made for these records in the Bill, we would be compelled to retain our records on paper files. We are reluctant to contemplate this; computerisation could improve the efficiency of our storage and retrieval of these records considerably. It is particularly difficult for our Appointments Unit, who deal both with judicial appointments and other Crown appointments, to discern the basis for distinguishing between the two.

Mrs Thatcher has therefore asked me to seek your advice on whether it might be possible to amend the Data Protection Bill to provide an exemption for records of honours and appointments similar to that provided for judicial appointments in Clause 30 of the Bill. She recognises that amendments for this purpose, and particularly for recommendations for honours, are likely to attract attention and no doubt opposition in some quarters in Parliament. Nevertheless there is a strong case for the exemption of recommendations for honours as those on the Opposition side, who have maintained a system of honours when they were in Government, must surely concede. The same applies to Crown appointments to which many of the same considerations which led the Lord Chancellor to press for an exemption for judicial appointments are also relevant.

AH

I apologise for raising this matter at this stage: as you know we did not have the chance of considering it when the Bill was being drafted.

I should be ready to discuss it with your officials should you think that desirable in view of the progress of the Committee Stage of the Bill in the House of Lords.

I am copying this letter to Sir Robert Armstrong.

Yours ever,

Robin Butler

John Halliday Esq.,
Home Office.

*see folder
in file*

Tim
Many thanks. If you are happy with my amendments, pl. fill in gaps in the first sentence & have typed for my signature
Robin
TFRS

DRAFT LETTER FROM MR. BUTLER TO MR. J. HALLIDAY, HOME OFFICE

DATA PROTECTION BILL

Tim Flesher wrote to Lesley Pallett on 8 December
~~In her letter to Tim Flesher of 17 December~~ about the implications for No. 10 of the Data Protection Bill ~~Lesley Pallett~~
about which we had not been previously consulted. In her reply of 17 December Lesley Pallett she
L said that it would be difficult to exempt the kind of material held here from the provisions of the Bill. I have now had a chance to discuss this with the Prime Minister and I fear that I must seek your advice once again.

As you know, the only material currently held on computer at No. 10 is that connected with our correspondence system. This system holds only such information as the names and addresses of the Prime Minister's correspondents and microfilmed records of their letters. We see no difficulty in giving the subjects of such data access to it, as required by the Bill. We could not, however, contemplate giving ^{similar} ~~such~~ access to the subjects of the records which we hold on honours and Crown appointments.

✓ In these circumstances, unless an exemption were made for these records in the Bill, we would be compelled to retain our records on paper files. ~~The Prime Minister is, however,~~ ^{we are} reluctant to contemplate this; computerisation could improve the efficiency of our storage and retrieval of these records considerably. ~~Mereover, she considers that it is important to establish the principle that records on honours and Crown appointments should remain confidential.~~ ^{It is particularly difficult for our Appointment Unit, who deal both with judicial appointments and other Crown appointments, to discern the basis for distinguishing between the two.} Mrs. Thatcher has therefore asked me to ^{seek your advice on} ~~enquire~~ whether it might be possible to

/amend

amend the Data Protection Bill to provide a ~~similar~~ exemption for records of honours and appointments ^{similar to that} in the same way as is provided for judicial appointments in Clause 30 of the Bill.

~~She~~ ^{She} & recognises ~~the difficulties which this request may pose for you at such a relatively late stage of the Bill's passage, although I should say that the point was not raised with us during the consultations which led to the drafting of the Bill.~~

~~I recognise, too, that the inclusion of an exemption for honours, may give rise to considerable opposition in some quarters. Nevertheless, I believe that there is a strong case on the merits for the exemption of honours as those on the Opposition side, who are not opposed in principle to an honours system and who indeed run one, must surely concede. The same, I believe, applies to Crown appointments to which many of the same considerations which led the Lord Chancellor to press for an exemption for judicial appointments~~ ^{are also relevant} apply.

~~I apologise for raising this matter at this stage: as you know we did not have the chance of considering it when the Bill was being drafted. It is now urgent~~

~~There is, of course, some urgency about this question in view of the imminence of the Committee Stage of the Bill in the House of Lords and my colleagues and I are ready to discuss it with your officials should you think that desirable in~~

I am copying this letter to Sir Robert Armstrong.

Herne Ogden

PRIME MINISTER

DATA PROTECTION BILL : HONOURS AND APPOINTMENTS

As you know, the Data Protection Bill is awaiting Committee Stage in the Lords. Amongst other things, the Bill provides that an individual shall be entitled to be informed by a user of data of whether such data includes personal information about him and to receive a copy of any such information. There are exemptions in the Bill for:

- i) national security
- ii) prevention or detection of crime
- iii) the apprehension or prosecution of offenders
- iv) the assessment or collection of any tax or duty
- v) the control of immigration
- vi) data on the physical or mental health of the subject
- vii) judicial appointments

The Bill has implications for No 10. We already have put records of correspondence on computer and the Bill will require us to give subjects of such data access to it. Since this will only mean giving writers of letters access to the records of their own correspondence, it is not likely to create any problems. What would create difficulties is if honours and appointments records were put on a similar computer system. This is a nuisance because I think that there may well be considerable scope for improving the efficiency of our storage and retrieval of these records by introducing a computer system.

As regards honours, we could not contemplate allowing the subject of honours recommendations access to the records about them: unless we can preserve the confidentiality of nominations and comments on the nominations, the honours system would be destroyed.

The same is true of information provided by third parties on Crown appointments: for Robin Catford's unit, it is nonsense

that the Bill should contain an exemption for information on judicial appointments but no exemption for the other Crown appointments with which they deal.

We have two options:-

- i) to seek an exemption from the provisions of the Data Protection Bill for honours and Crown appointments in the same way as the Lord Chancellor has secured one for judicial appointments - not easy, especially since an amendment to the Bill would now be necessary (although I expect that it should be easier to insert such amendments in the Lords, who are taking the Bill first, than in the Commons);
- ii) to continue to hold honours and appointments records on paper files and to abandon any notion of putting them on a computer: I see that Sir Robert Armstrong has said of the effect of the Bill on senior appointments in the Civil Service "I have taken the view that we shall simply have to continue to keep the records manually".

I recommend option (i), notwithstanding the difficulties: it would be a great pity to abandon the prospect of a more efficient system for holding and retrieving our records on honours and appointments.

I suggest therefore, if you agree, that I write to the Home Office seeking an exemption in the Bill for honours and crown appointments records, and propose that an amendment to the Bill be introduced in the House of Lords for this purpose. Do you agree ?

*I think we might
seek their advice. It is
the 'honours' aspect that is
likely to give rise to difficulty in
detail. We should be able to get
Crown Appointments through. not*

F.R.B.

8 February 1983

MR. BUTLER

DATA PROTECTION

I am conscious of having neglected this subject since our exchanges at the beginning of the year. I think that we ought to decide now whether we are going to take up the issue of whether to seek exemption for honours records from the provisions of the Data Protection Bill. You already know these, but to recap: under the Bill (Clause 21): "An individual shall be entitled to be informed by any data user whether the data held by him includes personal data of which that individual is the data subject" and "to be supplied by any data user with a copy in writing of the information constituting any such personal data held by him". There are a number of qualifications, but this is as close to being a right as makes no difference.

We have agreed that such a right for honours would be unacceptable. We have therefore two options:

- (i) to seek an exemption in the Bill for honours records; or
- (ii) to retain honours records on paper files and hope that the principle of data protection does not extend that far.

I prefer option (i) since we can always fall back on expediency if that fails. Moreover, an exemption for honours would I think be relatively easy to incorporate in the Bill. Clause 30, a copy of which is attached, makes an exemption for judicial appointments. That clause could simply be amended, for example, by the addition of the words at the end: "and the granting of honours by the Crown" or something along those lines.

If you agree, the question remains of how to proceed. I think we should put the matter to the Prime Minister to obtain her authority for an approach to the Home Secretary, and I

/ suggest

suggest that such an approach should be at Private Secretary level in the first instance.

A note canvassing the options for the Prime Minister is attached. If we are going to move we should do so quickly, because the Bill is now awaiting its Committee Stage in the Lords, which would be the most convenient time for an amendment.

I also considered whether we should seek an exemption for appointments. I believe that there is a strong case for this, but to some extent the pass has already been sold by Sir Robert Armstrong's letter of 8 December, copy attached, which abjures any exemption for Government appointments. It may be that Mr. Catford would wish to press the case for Church appointments and on this point he will know far more than I. Prima facie I cannot see a real distinction between clerical and judicial appointments justifying different treatment.

I am sending copies of this minute to Robin Catford, Joan Porter and Daphne Edmunds. Perhaps we could discuss this urgently in view of the stage at which the Bill is in the Lords.

JF

8 February 1983

Home Affairs
Data Protection
File

PART II

(4) Subject to subsection (5) below, the court by or before which a person is convicted of an offence under section 5, 10, 12 or 15 above may order any data material appearing to the court to be connected with the commission of the offence to be 5 forfeited, destroyed or erased.

(5) The court shall not make an order under subsection (4) above in relation to any material where a person (other than the offender) claiming to be the owner or otherwise interested in it applies to be heard by the court unless an opportunity is given 10 to him to show cause why the order should not be made.

20.—(1) Where an offence under this Part of this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or 15 similar officer of the body corporate or any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by 20 its members subsection (1) above shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

PART III

RIGHTS OF DATA SUBJECTS

25 21.—(1) Subject to the provisions of this section, an individual shall be entitled— Right of access to personal data.

(a) to be informed by any data user whether the data held by him includes personal data of which that individual is the data subject; and

30 (b) to be supplied by any data user with a copy in writing of the information constituting any such personal data held by him.

(2) A data user shall not be obliged to supply any information as aforesaid except in response to a request in writing and 35 on payment of such fee (not exceeding the prescribed maximum) as he may require.

(3) In the case of a data user having separate entries in the register in respect of data held for different purposes a separate request must be made and a separate fee paid under this section 40 in respect of the data to which each entry relates.

PART III

(4) A data user shall not be obliged to comply with a request under this section—

- (a) unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which he seeks ; and 5
- (b) if he cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request. 10

(5) In paragraph (b) of subsection (4) above the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request ; and that paragraph shall not be construed as excusing a data user from supplying so much of the information sought by the request as can be supplied without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise. 20

(6) A data user shall comply with a request under this section within twenty-eight days of receiving the request or, if later, receiving the information referred to in paragraph (a) of subsection (4) above and, in a case where it is required, the consent referred to in paragraph (b) of that subsection. 25

(7) The information to be supplied pursuant to a request under this section shall be supplied by reference to the data in question at the time when the request is received except that it may take account of any amendment made between that time and the time when the information is supplied, being an amendment for keeping the data accurate and up to date and made by virtue of instructions stored for automatic processing before the receipt of the request. 30

(8) 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 user in question has failed to comply with the request in contravention of those provisions, the court may order him to comply with the request ; but a court shall not make an order under this subsection if it considers that it would in all the circumstances be unreasonable to do so. 40

(9) The Secretary of State may by order provide for enabling a request under this section to be made on behalf of any individual who is incapable by reason of mental disorder of managing his own affairs.

22.—(1) A data subject who suffers damage by reason of the inaccuracy of personal data held by a data user shall be entitled to compensation for that damage from the data user.

PART III
Compensation
for
inaccuracy.

(2) In proceedings brought against any person by virtue of this section it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to ensure the accuracy of the data at the material time.

(3) For the purposes of this section data are inaccurate if incorrect or misleading as to any matter of fact, but data accurately recording information received or obtained by the data user from the data subject or a third party and indicating that it consists of such information shall not be regarded as inaccurate because that information was itself incorrect or misleading.

23.—(1) A data subject who suffers damage by reason of—

Compensation
for loss or
unauthorised
disclosure.

(a) the loss of personal data held by a data user or of personal data in respect of which services are provided by person carrying on a computer bureau ;

(b) the destruction of any such data without the authority of the data user or, as the case may be, of the person carrying on the bureau ; or

(c) subject to subsection (2) below, the disclosure of any such data without such authority as aforesaid,

shall be entitled to compensation for that damage from the data user or, as the case may be, the person carrying on the bureau.

(2) In the case of a registered data user, subsection (1)(c) above does not apply to disclosure to any person falling within a description specified in that behalf in an entry in the register relating to that data user.

(3) In proceedings brought against any person by virtue of this section it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to prevent the loss, destruction or disclosure in question.

24.—(1) If a court is satisfied on the application of a data subject—

Rectification
and erasure.

(a) that he has suffered damage by reason of the inaccuracy of personal data in circumstances entitling him to compensation under section 22 above ; or

(b) that he has suffered damage by reason of the disclosure of personal data in circumstances entitling him to compensation under section 23 above and that there is a substantial risk of further unauthorised disclosure,

PART III the court may order the rectification or erasure of the data and, in a case within paragraph (a) above, make such further order, if any, as it thinks just in respect of any other data appearing to the court to be based on the inaccurate data.

Jurisdiction. 25. The jurisdiction conferred by sections 21 and 24 above shall be exercisable by the High Court or a county court or, in Scotland, by the Court of Session or the sheriff. 5

PART IV

EXEMPTIONS

Preliminary. 26.—(1) References in any provision of Part II or III of this Act to personal data do not include references to data which by virtue of this Part of this Act are exempt from that provision. 10

(2) In this Part of this Act “the subject access provisions” means— 15

(a) section 21 above ; and

(b) any provision of Part II of this Act conferring a power on the Registrar to the extent to which it is exercisable by reference to the seventh data protection principle.

(3) In this Part of this Act “the non-disclosure provisions” means— 20

(a) sections 5(2)(d) and 15 above ; and

(b) any provision of Part II of this Act conferring a power on the Registrar to the extent to which it is exercisable by reference to any data protection principle inconsistent with the disclosure in question. 25

(4) Except as provided by this Part of this Act the subject access provisions shall apply notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information. 30

National security.

27.—(1) Personal data held by a government department are exempt from the provisions of Parts II and III of this Act if a Minister of the Crown certifies that the exemption is required for the purpose of safeguarding national security.

(2) Personal data held otherwise than by a government department are exempt from those provisions if held for the purpose of safeguarding national security. 35

(3) Personal data held otherwise than for the purpose of safeguarding national security are exempt from the non-disclosure provisions in any case in which the disclosure of the data is for that purpose.

PART IV

5 (4) For the purposes of subsections (2) and (3) above a certificate signed by or on behalf of a Minister of the Crown and certifying that personal data are or have been held or disclosed for the purpose of safeguarding national security shall be conclusive evidence of that fact.

10 (5) A document purporting to be such a certificate as is mentioned in this section shall be received in evidence and deemed to be such a certificate unless the contrary is proved.

28.—(1) Personal data held for any of the following purposes—

Crime,
taxation and
immigration
control.

- 15 (a) the prevention or detection of crime ;
(b) the apprehension or prosecution of offenders ;
(c) the assessment or collection of any tax or duty ; or
(d) the control of immigration,

20 are exempt from the subject access provisions in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data are exempt from the non-disclosure provisions in any case in which—

- 25 (a) the disclosure is for any of the purposes mentioned in subsection (1) above ; and
(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection ;

30 and in proceedings against any person for contravening a provision mentioned in section 26(3)(a) above it shall be a defence to prove that he had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those matters.

35 (3) Personal data are exempt from the provisions mentioned in subsection (4) below in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in subsection (1) above.

40 (4) The provisions referred to in subsection (3) above are the provisions of Part II of this Act conferring powers on the Registrar to the extent to which they are exercisable by reference to the first data protection principle.

PART IV
Health and
social work.

29.—(1) The Secretary of State may by order exempt from the subject access provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health of the data subject.

(2) The Secretary of State may by order exempt from the subject access provisions, or modify those provisions in relation to, personal data of such other descriptions as may be specified in the order, being information—

(a) held by government departments or local authorities or by voluntary organisations or other bodies designated by or under the order; and

(b) appearing to him to be held for, or acquired in the course of, carrying out social work in relation to the data subject or other individuals;

but the Secretary of State shall not under this subsection confer any exemption or make any modification except so far as he considers that those provisions (or those provisions without modification) would be likely to prejudice the carrying out of that work.

(3) An order under this section may make different provision in relation to data consisting of information of different descriptions.

Judicial
appointments.

30. Personal data held by a government department are exempt from the subject access provisions if the data consist of information which has been received from a third party and is held as information relevant to the making of judicial appointments.

Domestic
or other
limited
purposes.

31.—(1) Personal data held by an individual and concerned only with the management of his personal, family or household affairs are exempt from the provisions of Parts II and III of this Act.

(2) Subject to subsection (3) below—

(a) personal data held by an unincorporated members' club and relating only to the members of the club; and

(b) personal data held only for the purpose of distributing, or recording the distribution of, articles to the data subjects and consisting only of their names and addresses,

are exempt from the provisions of Parts II and III of this Act.

(3) Neither paragraph (a) nor paragraph (b) of subsection (2) above applies to personal data relating to any data subject unless he has been asked whether he objects to the data relating to him being held as mentioned in that paragraph and has not objected.

32.—(1) The Secretary of State may by order exempt from the subject access provisions personal data consisting of information—

PART IV
Other
exemptions.

5 (a) the disclosure of which is prohibited or restricted by or under any enactment ; and

10 (b) which appears to him to be of such a nature that its confidentiality ought to be preserved or that the provisions prohibiting or restricting its disclosure ought for any other reason to prevail over the subject access provisions.

(2) Personal data are exempt from the subject access provisions if the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

15 (3) Personal data held only for—

(a) preparing statistics ; or

(b) carrying out research,

20 are exempt from the subject access provisions unless the resulting statistics or the results of the research are made available in a form which identifies the data subjects or any of them.

(4) Personal data are exempt from the non-disclosure provisions in any case in which—

(a) the data subject has requested or consented to the particular disclosure in question ; or

25 (b) the disclosure is required by or under any enactment or by the order of a court.

30 (5) Personal data are exempt from the non-disclosure provisions in any case in which the disclosure is urgently required for preventing injury or other damage to the health of any person or persons ; and in proceedings against any person for contravening a provision mentioned in section 26(3)(a) above it shall be a defence to prove that he had reasonable grounds for believing that the disclosure in question was urgently required for that purpose.

35 (6) A person need not comply with a notice, request or order under the subject access provisions if compliance would expose him to proceedings for any offence other than an offence under Part II of this Act ; and information disclosed by any person in compliance with such a notice, request or order shall not be
40 admissible against him in proceedings for an offence under that Part.



Home Off
HOME OFFICE
QUEEN ANNE'S GATE
LONDON SW1H 9AT

1.17
20/12

20th December, 1982

Dear de Waal,

DATA PROTECTION BILL

As you know this Bill is to be considered by the Legislation Committee tomorrow morning, Tuesday, 21st December. We are hopeful that the Committee will approve the immediate introduction of the Bill, in which case I should be grateful if you would arrange for the introduction of the Bill in the name of Lord Elton in the House of Lords tomorrow afternoon, with publication by 11 a.m on Wednesday, 22nd December.

We are not having a Press Conference at the time of publication but there will be some press briefing and it would be helpful if 80 copies of the Bill addressed to Lord Elton could be available in the Printed Paper Office at the time of publication.

I am sending copies of this letter to Willie Rickett (Prime Minister's Office), Leonard Harris (Cabinet Office), David Heyhoe (Lord President's Office), Murdo Maclean (Chief Whip's Office, Commons), Michael Pownall (Chief Whip's Office, Lords) and Brian Shillito.

Yours sincerely,
T. C. Morris

T. C. MORRIS
Parliamentary Clerk

C. H. de Waal Esq., C.B.

MR CATFORD

^B
~~Miss Brewer~~ to see
~~Miss Parker~~ to discuss, please,
after Christmas. *OK* 22/12

DATA PROTECTION

You may be interested to see the attached correspondence between myself and the Home Office about the implications for this office of the Data Protection Bill. I also enclose a copy of those provisions of the Bill which will bear upon us should our honours and appointments records be computerised. The correspondence is self-explanatory and my note of 17 December sets out what I think are the main considerations. As you will see, Robin Butler has asked that we should have a word at some stage.

Tf.

20 December, 1982

MR BUTLER

DATA PROTECTION

You asked that we should have a word about the implications of the Data Protection Bill for this office and I have given Robin Catford a copy of the relevant correspondence.

You may be interested to see as a preliminary to our discussion the attached copy of the relevant provisions of the Data Protection Bill. The reason for the Bill is to enable the United Kingdom to ratify the Council of Europe Convention on Data Protection which is thought to be essential to the protection of our data industry. A particular need is to guard against the possibility of countries which already have data protection legislation prohibiting the transfer of personal data to the United Kingdom. In domestic political terms the Bill is to meet the widespread concern of those particular risks to privacy from the ability of computers rapidly to process and retrieve data held in such a way.

The Bill provides that an individual shall be entitled to be informed by a data user of whether that data includes personal information about him and to receive a copy of such information. The exemptions are for:-

- (i) national security;
- (ii) the prevention or detection of crime;
- (iii) the apprehension or prosecution of offenders;
- (iv) the assessment or collection of any tax or duty;
- (v) the control of immigration;
- (vi) data on the physical or mental health of the subject;

/(vii)

(vii) data relating to judicial appointments.

Several of these exemptions will be challenged in the House possibly successfully. There is, moreover, likely to be an attempt to extend the right of access provisions to paper files. There is probably a majority in the House in favour of this kind of legislation and the distinction between data held on paper files is politically attractive but intellectually untenable.

TF.

20 December, 1982

PART II

(4) Subject to subsection (5) below, the court by or before which a person is convicted of an offence under section 5, 10, 12 or 15 above may order any data material appearing to the court to be connected with the commission of the offence to be forfeited, destroyed or erased.

(5) The court shall not make an order under subsection (4) above in relation to any material where a person (other than the offender) claiming to be the owner or otherwise interested in it applies to be heard by the court unless an opportunity is given to him to show cause why the order should not be made.

20.—(1) Where an offence under this Part of this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members subsection (1) above shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

PART III

RIGHTS OF DATA SUBJECTS

21.—(1) Subject to the provisions of this section, an individual shall be entitled—
(a) to be informed by any data user whether the data held by him includes personal data of which that individual is the data subject; and

(b) to be supplied by any data user with a copy in writing of the information constituting any such personal data held by him.

(2) A data user shall not be obliged to supply any information as aforesaid except in response to a request in writing and on payment of such fee (not exceeding the prescribed maximum) as he may require.

(3) In the case of a data user having separate entries in the register in respect of data held for different purposes a separate request must be made and a separate fee paid under this section in respect of the data to which each entry relates.

PART III

(4) A data user shall not be obliged to comply with a request under this section—

- (a) unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which he seeks ; and 5
- (b) if he cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request. 10

(5) In paragraph (b) of subsection (4) above the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request ; and that paragraph shall not be construed as excusing a data user from supplying so much of the information sought by the request as can be supplied without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise. 20

(6) A data user shall comply with a request under this section within twenty-eight days of receiving the request or, if later, receiving the information referred to in paragraph (a) of subsection (4) above and, in a case where it is required, the consent referred to in paragraph (b) of that subsection. 25

(7) The information to be supplied pursuant to a request under this section shall be supplied by reference to the data in question at the time when the request is received except that it may take account of any amendment made between that time and the time when the information is supplied, being an amendment for keeping the data accurate and up to date and made by virtue of instructions stored for automatic processing before the receipt of the request. 30

(8) 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 user in question has failed to comply with the request in contravention of those provisions, the court may order him to comply with the request ; but a court shall not make an order under this subsection if it considers that it would in all the circumstances be unreasonable to do so. 40

(9) The Secretary of State may by order provide for enabling a request under this section to be made on behalf of any individual who is incapable by reason of mental disorder of managing his own affairs.

22.—(1) A data subject who suffers damage by reason of the inaccuracy of personal data held by a data user shall be entitled to compensation for that damage from the data user.

PART III
Compensation
for
inaccuracy.

(2) In proceedings brought against any person by virtue of this section it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to ensure the accuracy of the data at the material time.

(3) For the purposes of this section data are inaccurate if incorrect or misleading as to any matter of fact, but data accurately recording information received or obtained by the data user from the data subject or a third party and indicating that it consists of such information shall not be regarded as inaccurate because that information was itself incorrect or misleading.

23.—(1) A data subject who suffers damage by reason of—

Compensation
for loss or
unauthorised
disclosure.

(a) the loss of personal data held by a data user or of personal data in respect of which services are provided by person carrying on a computer bureau ;

(b) the destruction of any such data without the authority of the data user or, as the case may be, of the person carrying on the bureau ; or

(c) subject to subsection (2) below, the disclosure of any such data without such authority as aforesaid,

shall be entitled to compensation for that damage from the data user or, as the case may be, the person carrying on the bureau.

(2) In the case of a registered data user, subsection (1)(c) above does not apply to disclosure to any person falling within a description specified in that behalf in an entry in the register relating to that data user.

(3) In proceedings brought against any person by virtue of this section it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to prevent the loss, destruction or disclosure in question.

24.—(1) If a court is satisfied on the application of a data subject—

Rectification
and erasure.

(a) that he has suffered damage by reason of the inaccuracy of personal data in circumstances entitling him to compensation under section 22 above ; or

(b) that he has suffered damage by reason of the disclosure of personal data in circumstances entitling him to compensation under section 23 above and that there is a substantial risk of further unauthorised disclosure,

PART III the court may order the rectification or erasure of the data and, in a case within paragraph (a) above, make such further order, if any, as it thinks just in respect of any other data appearing to the court to be based on the inaccurate data.

Jurisdiction. 25. The jurisdiction conferred by sections 21 and 24 above shall be exercisable by the High Court or a county court or, in Scotland, by the Court of Session or the sheriff. 5

PART IV

EXEMPTIONS

Preliminary. 26.—(1) References in any provision of Part II or III of this Act to personal data do not include references to data which by virtue of this Part of this Act are exempt from that provision. 10

(2) In this Part of this Act “the subject access provisions” means— 15

(a) section 21 above ; and

(b) any provision of Part II of this Act conferring a power on the Registrar to the extent to which it is exercisable by reference to the seventh data protection principle.

(3) In this Part of this Act “the non-disclosure provisions” means— 20

(a) sections 5(2)(d) and 15 above ; and

(b) any provision of Part II of this Act conferring a power on the Registrar to the extent to which it is exercisable by reference to any data protection principle inconsistent with the disclosure in question. 25

(4) Except as provided by this Part of this Act the subject access provisions shall apply notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information. 30

National security.

27.—(1) Personal data held by a government department are exempt from the provisions of Parts II and III of this Act if a Minister of the Crown certifies that the exemption is required for the purpose of safeguarding national security.

(2) Personal data held otherwise than by a government department are exempt from those provisions if held for the purpose of safeguarding national security. 35

(3) Personal data held otherwise than for the purpose of safeguarding national security are exempt from the non-disclosure provisions in any case in which the disclosure of the data is for that purpose.

5 (4) For the purposes of subsections (2) and (3) above a certificate signed by or on behalf of a Minister of the Crown and certifying that personal data are or have been held or disclosed for the purpose of safeguarding national security shall be conclusive evidence of that fact.

10 (5) A document purporting to be such a certificate as is mentioned in this section shall be received in evidence and deemed to be such a certificate unless the contrary is proved.

28.—(1) Personal data held for any of the following purposes—

- 15 (a) the prevention or detection of crime ;
 (b) the apprehension or prosecution of offenders ;
 (c) the assessment or collection of any tax or duty ; or
 (d) the control of immigration,

Crime,
taxation and
immigration
control.

20 are exempt from the subject access provisions in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data are exempt from the non-disclosure provisions in any case in which—

- 25 (a) the disclosure is for any of the purposes mentioned in subsection (1) above ; and
 (b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection ;

30 and in proceedings against any person for contravening a provision mentioned in section 26(3)(a) above it shall be a defence to prove that he had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those matters.

35 (3) Personal data are exempt from the provisions mentioned in subsection (4) below in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in subsection (1) above.

40 (4) The provisions referred to in subsection (3) above are the provisions of Part II of this Act conferring powers on the Registrar to the extent to which they are exercisable by reference to the first data protection principle.

PART IV
Health and
social work.

29.—(1) The Secretary of State may by order exempt from the subject access provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health of the data subject.

(2) The Secretary of State may by order exempt from the subject access provisions, or modify those provisions in relation to, personal data of such other descriptions as may be specified in the order, being information—

(a) held by government departments or local authorities or by voluntary organisations or other bodies designated by or under the order ; and

(b) appearing to him to be held for, or acquired in the course of, carrying out social work in relation to the data subject or other individuals ;

but the Secretary of State shall not under this subsection confer any exemption or make any modification except so far as he considers that those provisions (or those provisions without modification) would be likely to prejudice the carrying out of that work.

(3) An order under this section may make different provision in relation to data consisting of information of different descriptions.

Judicial
appointments.

30. Personal data held by a government department are exempt from the subject access provisions if the data consist of information which has been received from a third party and is held as information relevant to the making of judicial appointments.

Domestic
or other
limited
purposes.

31.—(1) Personal data held by an individual and concerned only with the management of his personal, family or household affairs are exempt from the provisions of Parts II and III of this Act.

(2) Subject to subsection (3) below—

(a) personal data held by an unincorporated members' club and relating only to the members of the club ; and

(b) personal data held only for the purpose of distributing, or recording the distribution of, articles to the data subjects and consisting only of their names and addresses,

are exempt from the provisions of Parts II and III of this Act.

(3) Neither paragraph (a) nor paragraph (b) of subsection (2) above applies to personal data relating to any data subject unless he has been asked whether he objects to the data relating to him being held as mentioned in that paragraph and has not objected.

32.—(1) The Secretary of State may by order exempt from the subject access provisions personal data consisting of information—

PART IV
Other
exemptions.

- 5 (a) the disclosure of which is prohibited or restricted by or under any enactment ; and
- 10 (b) which appears to him to be of such a nature that its confidentiality ought to be preserved or that the provisions prohibiting or restricting its disclosure ought for any other reason to prevail over the subject access provisions.

(2) Personal data are exempt from the subject access provisions if the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

15 (3) Personal data held only for—

- (a) preparing statistics ; or
(b) carrying out research,

are exempt from the subject access provisions unless the resulting statistics or the results of the research are made available
20 in a form which identifies the data subjects or any of them.

(4) Personal data are exempt from the non-disclosure provisions in any case in which—

- 25 (a) the data subject has requested or consented to the particular disclosure in question ; or
(b) the disclosure is required by or under any enactment or by the order of a court.

30 (5) Personal data are exempt from the non-disclosure provisions in any case in which the disclosure is urgently required for preventing injury or other damage to the health of any person or persons ; and in proceedings against any person for contravening a provision mentioned in section 26(3)(a) above it shall be a defence to prove that he had reasonable grounds for believing that the disclosure in question was urgently required for that purpose.

35 (6) A person need not comply with a notice, request or order under the subject access provisions if compliance would expose him to proceedings for any offence other than an offence under Part II of this Act ; and information disclosed by any person in compliance with such a notice, request or order shall not be
40 admissible against him in proceedings for an offence under that Part.

Le



HOME OFFICE
QUEEN ANNE'S GATE
LONDON SW1H 9AT

17 December 1982

Dear Tim,

DATA PROTECTION BILL

Thank you for your letter of 8 December.

I fear that I must confirm your view that it would be extremely difficult to make special provision in the Bill to exempt the kind of data that you hold at No.10. This means either that the particularly sensitive data are not put onto a computer (much of your material is, of course, straightforward factual information which presumably poses no problems) or that the computerised records comply with the provisions of the Bill, including the requirement to give subject access.

You may be aware that Sir Robert Armstrong has written to Sir Brian Cubbon making clear his view that special exemptions cannot be given in the Bill to data concerning senior appointments in the Civil Service. If necessary, certain data will have to continue to be held manually. However, the Lord Chancellor (as the attached copies of recent correspondence show) does hold to the view that judicial appointments can be distinguished from other senior appointments and that exemption is essential. On that basis the Home Secretary has accepted that an exemption limited to judicial appointments should be included in the Bill. That in itself will be difficult enough to defend. To take the exemption any wider would greatly multiply the difficulties.

I am copying this letter to Richard Hatfield.

Yours sincerely,

Lesley Pallett.

MRS L PALLETT

T. J. Flesher, Esq.

(4) Subject to subsection (5) below, the court by or before which a person is convicted of an offence under section 5, 10, 12 or 15 above may order any data material appearing to the court to be connected with the commission of the offence to be forfeited, destroyed or erased.

PART II

(5) The court shall not make an order under subsection (4) above in relation to any material where a person (other than the offender) claiming to be the owner or otherwise interested in it applies to be heard by the court unless an opportunity is given to him to show cause why the order should not be made.

20.—(1) Where an offence under this Part of this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

Liability of directors etc.

(2) Where the affairs of a body corporate are managed by its members subsection (1) above shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

PART III

RIGHTS OF DATA SUBJECTS

25 21.—(1) Subject to the provisions of this section, an individual shall be entitled—

Right of access to personal data.

(a) to be informed by any data user whether the data held by him includes personal data of which that individual is the data subject; and

30 (b) to be supplied by any data user with a copy in writing of the information constituting any such personal data held by him.

(2) A data user shall not be obliged to supply any information as aforesaid except in response to a request in writing and on payment of such fee (not exceeding the prescribed maximum) as he may require.

(3) In the case of a data user having separate entries in the register in respect of data held for different purposes a separate request must be made and a separate fee paid under this section in respect of the data to which each entry relates.

PART III

(4) A data user shall not be obliged to comply with a request under this section—

- (a) unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which he seeks ; and 5
- (b) if he cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request. 10

(5) In paragraph (b) of subsection (4) above the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request ; and that paragraph shall not be construed as excusing a data user from supplying so much of the information sought by the request as can be supplied without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise. 20

(6) A data user shall comply with a request under this section within twenty-eight days of receiving the request or, if later, receiving the information referred to in paragraph (a) of subsection (4) above and, in a case where it is required, the consent referred to in paragraph (b) of that subsection. 25

(7) The information to be supplied pursuant to a request under this section shall be supplied by reference to the data in question at the time when the request is received except that it may take account of any amendment made between that time and the time when the information is supplied, being an amendment for keeping the data accurate and up to date and made by virtue of instructions stored for automatic processing before the receipt of the request. 30

(8) 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 user in question has failed to comply with the request in contravention of those provisions, the court may order him to comply with the request ; but a court shall not make an order under this subsection if it considers that it would in all the circumstances be unreasonable to do so. 40

(9) The Secretary of State may by order provide for enabling a request under this section to be made on behalf of any individual who is incapable by reason of mental disorder of managing his own affairs.

22.—(1) A data subject who suffers damage by reason of the inaccuracy of personal data held by a data user shall be entitled to compensation for that damage from the data user.

PART III
Compensation
for
inaccuracy.

(2) In proceedings brought against any person by virtue of this section it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to ensure the accuracy of the data at the material time.

(3) For the purposes of this section data are inaccurate if incorrect or misleading as to any matter of fact, but data accurately recording information received or obtained by the data user from the data subject or a third party and indicating that it consists of such information shall not be regarded as inaccurate because that information was itself incorrect or misleading.

23.—(1) A data subject who suffers damage by reason of—

Compensation
for loss or
unauthorised
disclosure.

(a) the loss of personal data held by a data user or of personal data in respect of which services are provided by person carrying on a computer bureau ;

(b) the destruction of any such data without the authority of the data user or, as the case may be, of the person carrying on the bureau ; or

(c) subject to subsection (2) below, the disclosure of any such data without such authority as aforesaid,

shall be entitled to compensation for that damage from the data user or, as the case may be, the person carrying on the bureau.

(2) In the case of a registered data user, subsection (1)(c) above does not apply to disclosure to any person falling within a description specified in that behalf in an entry in the register relating to that data user.

(3) In proceedings brought against any person by virtue of this section it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to prevent the loss, destruction or disclosure in question.

24.—(1) If a court is satisfied on the application of a data subject—

Rectification
and erasure.

(a) that he has suffered damage by reason of the inaccuracy of personal data in circumstances entitling him to compensation under section 22 above ; or

(b) that he has suffered damage by reason of the disclosure of personal data in circumstances entitling him to compensation under section 23 above and that there is a substantial risk of further unauthorised disclosure,

PART III the court may order the rectification or erasure of the data and, in a case within paragraph (a) above, make such further order, if any, as it thinks just in respect of any other data appearing to the court to be based on the inaccurate data.

Jurisdiction. 25. The jurisdiction conferred by sections 21 and 24 above shall be exercisable by the High Court or a county court or, in Scotland, by the Court of Session or the sheriff. 5

PART IV

EXEMPTIONS

Preliminary. 26.—(1) References in any provision of Part II or III of this Act to personal data do not include references to data which by virtue of this Part of this Act are exempt from that provision. 10

(2) In this Part of this Act “the subject access provisions” means— 15

(a) section 21 above ; and

(b) any provision of Part II of this Act conferring a power on the Registrar to the extent to which it is exercisable by reference to the seventh data protection principle.

(3) In this Part of this Act “the non-disclosure provisions” means— 20

(a) sections 5(2)(d) and 15 above ; and

(b) any provision of Part II of this Act conferring a power on the Registrar to the extent to which it is exercisable by reference to any data protection principle inconsistent with the disclosure in question. 25

(4) Except as provided by this Part of this Act the subject access provisions shall apply notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information. 30

National security.

27.—(1) Personal data held by a government department are exempt from the provisions of Parts II and III of this Act if a Minister of the Crown certifies that the exemption is required for the purpose of safeguarding national security.

(2) Personal data held otherwise than by a government department are exempt from those provisions if held for the purpose of safeguarding national security. 35

(3) Personal data held otherwise than for the purpose of safeguarding national security are exempt from the non-disclosure provisions in any case in which the disclosure of the data is for that purpose.

5 (4) For the purposes of subsections (2) and (3) above a certificate signed by or on behalf of a Minister of the Crown and certifying that personal data are or have been held or disclosed for the purpose of safeguarding national security shall be conclusive evidence of that fact.

10 (5) A document purporting to be such a certificate as is mentioned in this section shall be received in evidence and deemed to be such a certificate unless the contrary is proved.

28.—(1) Personal data held for any of the following purposes—

- 15 (a) the prevention or detection of crime ;
 (b) the apprehension or prosecution of offenders ;
 (c) the assessment or collection of any tax or duty ; or
 (d) the control of immigration,

Crime,
 taxation and
 immigration
 control.

20 are exempt from the subject access provisions in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data are exempt from the non-disclosure provisions in any case in which—

- 25 (a) the disclosure is for any of the purposes mentioned in subsection (1) above ; and
 (b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection ;

30 and in proceedings against any person for contravening a provision mentioned in section 26(3)(a) above it shall be a defence to prove that he had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those matters.

35 (3) Personal data are exempt from the provisions mentioned in subsection (4) below in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in subsection (1) above.

40 (4) The provisions referred to in subsection (3) above are the provisions of Part II of this Act conferring powers on the Registrar to the extent to which they are exercisable by reference to the first data protection principle.

PART IV
Health and
social work.

29.—(1) The Secretary of State may by order exempt from the subject access provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health of the data subject.

(2) The Secretary of State may by order exempt from the subject access provisions, or modify those provisions in relation to, personal data of such other descriptions as may be specified in the order, being information—

(a) held by government departments or local authorities or by voluntary organisations or other bodies designated by or under the order; and

(b) appearing to him to be held for, or acquired in the course of, carrying out social work in relation to the data subject or other individuals;

but the Secretary of State shall not under this subsection confer any exemption or make any modification except so far as he considers that those provisions (or those provisions without modification) would be likely to prejudice the carrying out of that work.

(3) An order under this section may make different provision in relation to data consisting of information of different descriptions.

Judicial
appointments.

30. Personal data held by a government department are exempt from the subject access provisions if the data consist of information which has been received from a third party and is held as information relevant to the making of judicial appointments.

Domestic
or other
limited
purposes.

31.—(1) Personal data held by an individual and concerned only with the management of his personal, family or household affairs are exempt from the provisions of Parts II and III of this Act.

(2) Subject to subsection (3) below—

(a) personal data held by an unincorporated members' club and relating only to the members of the club; and

(b) personal data held only for the purpose of distributing, or recording the distribution of, articles to the data subjects and consisting only of their names and addresses,

are exempt from the provisions of Parts II and III of this Act.

(3) Neither paragraph (a) nor paragraph (b) of subsection (2) above applies to personal data relating to any data subject unless he has been asked whether he objects to the data relating to him being held as mentioned in that paragraph and has not objected.

32.—(1) The Secretary of State may by order exempt from the subject access provisions personal data consisting of information—

PART IV
Other
exemptions.

- 5 (a) the disclosure of which is prohibited or restricted by or under any enactment ; and
- 10 (b) which appears to him to be of such a nature that its confidentiality ought to be preserved or that the provisions prohibiting or restricting its disclosure ought for any other reason to prevail over the subject access provisions.

(2) Personal data are exempt from the subject access provisions if the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

15 (3) Personal data held only for—

- (a) preparing statistics ; or
- (b) carrying out research,

are exempt from the subject access provisions unless the resulting statistics or the results of the research are made available in a form which identifies the data subjects or any of them.

(4) Personal data are exempt from the non-disclosure provisions in any case in which—

- 25 (a) the data subject has requested or consented to the particular disclosure in question ; or
- (b) the disclosure is required by or under any enactment or by the order of a court.

30 (5) Personal data are exempt from the non-disclosure provisions in any case in which the disclosure is urgently required for preventing injury or other damage to the health of any person or persons ; and in proceedings against any person for contravening a provision mentioned in section 26(3)(a) above it shall be a defence to prove that he had reasonable grounds for believing that the disclosure in question was urgently required for that purpose.

35 (6) A person need not comply with a notice, request or order under the subject access provisions if compliance would expose him to proceedings for any offence other than an offence under Part II of this Act ; and information disclosed by any person in compliance with such a notice, request or order shall not be

40 admissible against him in proceedings for an offence under that Part.

MR BUTLER

Mr. Fleisher

Yes let us have a word. Mr. Catford should also be involved. You will have to explain to me what ~~are~~ the arguments for giving people this ^{sort of access} DATA PROTECTION ~~FILES~~

18.12

You may be interested to see the attached letter from the Home Office which follows my inquiry about the status of our honours and appointments records in relation to the Data Protection Bill. As you will see, the Home Secretary has agreed reluctantly to the Lord Chancellor's request that there should be an exemption in the Bill for judicial appointments; Sir Robert Armstrong has, however, indicated his view that Civil Service appointments cannot be exempted. On appointments I think that the Lord Chancellor's justification for distinctions between judicial and other Crown appointments is rather tenuous. I do not see, for example, that the processes involved in the appointment of a judge are in any real sense different from or more confidential than those involved in say the appointment of a chairman of a Royal Commission.

I think this applies to an even greater extent to honours. Although I do not have a detailed knowledge of the way in which the system of recommendations for honours are processed I cannot believe that it would not be widely accepted that these should be exempt from access by their subjects. Indeed, there would be little point in a system of honours with such access.

If you agree with the foregoing we have two choices. First, we could return to the charge and press the Home Secretary to accept a formal exemption in the Bill for honours records and possibly appointments, (although I am ^{less} ~~least~~ concerned about the latter). Such a course would be politically difficult but would at least have the advantage of establishing the principle that honours are different from other kinds of record. Second, we could simply accept that for the foreseeable future we could not computerise honours and appointments records. This is, of course, the line of least resistance but would effectively prevent us from thoroughly modernising our office practices. It is moreover entirely possible that we should have to fight the confidentiality battle at a later stage if there is ever an attempt to extend the data protection principle to manual records.

* But some of our appointments files are highly confidential, especially ^{Senior Church} ^{appts, hd-wts,} ^{Regius Professors} 2/12. /My

My preference is for the first course, if only to place our position on record. Can we discuss possibly with a view to consulting the Prime Minister?

JF

17 December, 1982



QUEEN ANNE'S GATE
LONDON SW1H 9AT

9 December 1982

Dear Garton

DATA PROTECTION BILL

Thank you for your letter of 8 December. I shall arrange for a provision on judicial appointments to be included in the Bill for Legislation Committee. We shall then have to see how the provision fares during the Bill's Parliamentary passage.

I am copying this letter to members of H Committee and to Sir Robert Armstrong.

M. Hailsham

The Rt. Hon. Lord Hailsham of St. Marylebone,
CH., FRS., DCL.

FROM:

THE RT. HON. LORD HAILSHAM OF ST. MARYLEBONE, C.H., F.R.S., D.C.L.



HOUSE OF LORDS,
SW1A 0PW

8th December, 1982

The Right Honourable
William Whitelaw, CH MC MP
Secretary of State for the Home Dept.,
Home Office,
Queen Anne's Gate,
London, SW1.

My dear Willie..

Data Protection Bill

Thank you for your letter of 7th December. I am grateful for the consideration that you and your officials have given to this, and glad that you accept that a suitable provision to meet my needs should be inserted in the Bill. Let us proceed as you propose.

Without going back over the arguments, I had better make it clear for the record (in view of what you say in your letter) that although I have not myself sought to make any distinction in principle between the records for which I am responsible relating to judicial appointments and others relating to other Crown appointments, I would find it possible to argue that in one sense they were different in that judicial officers constitute a separate branch of Government in accordance with the doctrine of the separation of powers, and that at all costs judicial appointments must be seen in a unique light. To this I add, and quite independently, that the records for which I am responsible cannot in any circumstances be shown to the subjects concerned, and that it would be extremely improvident to prevent ourselves forever putting it onto any kind of computer.

For these reasons, I am afraid I cannot agree to your suggestion that, if the provision upon which we have agreed were challenged or used as an argument for other proposed exemptions, it should be dropped.

I am copying this to members of H Committee and to Sir Robert Armstrong.

yrs.



cc - Mr. Flesher

Home Affairs

~~cc - Mr. Hilary
H. Peterson~~

MANAGEMENT AND PERSONNEL OFFICE

C	157	Whitehall, London SW1A 2AS Telephone 01-233 8319
From the Permanent Secretary: Sir Robert Armstrong KCB CVO		
Ref: 5 DEC 1982	A08276433	
FILE No.	

8 December 1982

*will request
if required*

14/12

Data Protection Bill

I have seen a copy of the Home Secretary's letter of 7 December about the possibility of including in the Data Protection Bill a provision exempting from subject access data relating to judicial appointments.

We have very similar problems and concerns in relation to senior appointments in the Civil Service. Material is held in my office and in the Management and Personnel Office which it could well be convenient at some time to put on to a computer. Many of the arguments for exempting judicial appointments would apply also to the appointments with which I am concerned. I have, however, taken the view that, if there is no comparable exemption for senior appointments in other walks of life, it would be very difficult to justify an exemption in respect of senior civil servants. I must say that I share the Home Secretary's view that it would be difficult to draw any valid distinction for this purpose between judicial appointments and other senior appointments in the public and private sectors. In respect of senior appointments in the Civil Service, I have taken the view that we shall simply have to continue to keep the records manually. I do not have much enthusiasm for the idea of making special provision for judicial appointments only, particularly if the Government would in practice be ready to drop the provision if it came under sustained challenge or query.

I am sending a copy of this letter to Derek Oulton.

ROBERT ARMSTRONG

Sir Brian Cubbon KCB

Home Affairs

Data Inductis

1/01 1960

CONFIDENTIAL



cc CO SW
Home Affairs

10 DOWNING STREET

From the Private Secretary

8 December, 1982

Dear Lesley,

I mentioned to you recently the position of No. 10 in relation to the Data Protection Bill. As you know, we have already installed a micro-computer system for records of the Prime Minister's correspondence which will hold approximately 150,000 names and addresses. For the future, we have been considering whether we might extend such a system to hold our honours and appointments records. At present these records are, of course, held on paper files. Clearly, these records are subject to the same considerations as judicial appointments, to which the Lord Chancellor drew attention at the meeting of H Committee on Monday, 29 November. Such is the need for confidentiality of these records that unless they could be exempt from the provisions of the Data Protection Bill on subject access, we should have to retain them in manual form.

B/F
I should be grateful if you could arrange to look into the position of our records, including those of correspondence, honours and appointments, in relation to the Bill and let me know whether, as I suspect, exemption would be as difficult for our records as H Committee decided it was for those of judicial appointments.

I am copying this to Richard Hatfield (Cabinet Office).

Yours ever,
Tim

TIMOTHY FLESHER

Mrs. Lesley Pallett,
Home Office

CONFIDENTIAL

JP



QUEEN ANNE'S GATE LONDON SW1H 9AT

7 December 1982

Dear Quintin

DATA PROTECTION BILL

Following discussion at H Committee on 29 November your officials and mine have given further consideration to the possibility of including in the Data Protection Bill a provision exempting from subject access data relating to judicial appointments.

You will not, I think, expect me to rehearse again the arguments against such a provision. I still cannot see how to draw any valid distinction for this purpose between judicial appointments and other senior appointments in the public and private sectors, many of which must be made on the basis of confidential reports by third parties.

From what I have heard about the sort of sensitive material you have in mind, my own preference would be not to put it on a computer at all. This would be the best protection both for your informants and for the people to whom the information relates.

We can approach the Bill only on the basis that the control of manual records is an entirely separate matter.

However, if you consider that it is desirable to put this highly sensitive material on a computer and it is accepted by our colleagues that judicial appointments can be regarded as sui generis for this purpose, I am prepared to agree that officials should consider with the draftsman, as a matter of urgency, how best an appropriate provision could be included in the Bill. Such a provision should be restricted to personal data received from a third party and relating to the suitability of a data subject for judicial office.

If we were pressed in the course of the Bill's passage through Parliament to justify this special provision for judicial appointments only, or to widen it to cover appointments generally, I am bound to say that I would be disposed to drop it altogether rather than widen its scope in such a way as to nullify one of the Bill's main safeguards (i.e. subject access) against inaccuracy or misuse of personal data held on computers.

I am copying this letter to members of H Committee and to Sir Robert Armstrong.

Yours truly,
William

PRIME MINISTER

DATA PROTECTION: H COMMITTEE DISCUSSION

Attached are the minutes of H Committee which discussed the Data Protection Bill. The Committee reluctantly agreed that police and tax records should be brought within the scope of the registration system proposed in the Bill subject only to restrictions on access by the subject and on disclosure. They did not agree that judicial appointments should be exempted from the provisions of the Bill and it was noted that material on a number of sensitive appointments and honours would have to be kept on paper files. This has, of course, implications for No.10. Although we have no proposals at present to put our honours and appointments records on computer we hope that this might be possible at some stage in the not too distant future. We could not, therefore, fall in with the requirement of the Bill on disclosure and access by subjects. I am exploring the position with the Home Office.

3 December, 1982

PRIME MINISTER

H Committee: Data Protection Bill

Attached are two papers which are being taken at H next week on the Data Protection Bill. The first, by the Home Secretary, proposes that data used for the prevention or detection of crime or the assessment and collection of tax should be subject to the same process of registration as other data instead of being exempt by Ministerial certificate in the same way as security information. Such information would continue to be exempt from the requirement to give subjects access to their data. This will not be popular with the police but the Home Secretary considers that the safeguards for them are adequate and that in any event without the change the Bill would be in Parliamentary danger.

The second paper, by the Lord Chancellor, asks for two more exemptions from the "Right to Know" provisions in the Bill. The first is information given to a legal adviser; the second is information on judicial appointments.

JF.

Tim Flesher

26 November 1982

SIR ROBERT ARMSTRONG

Many thanks for your minute of 12 November (AOS2/0094) about the article in The Times of 8 November claiming that a review of security methods used for computer-stored data banks had been ordered by the "Cabinet joint committee on intelligence". I have noted that the JIC has not ordered such a review and that this seems to be a garbled reference to the senior security committee on electronic information processing.

ROBIN BUTLER

16 November 1982

↙

010
Ref. A082/0094

MR BUTLER ✓

An article in The Times of 8 November by its Science Editor (copy attached) claimed that a review of security methods used for computer-stored data banks had been ordered by "the Cabinet joint committee on intelligence".

2. The JIC has not ordered any such review. This appears to be a garbled account of the decision, taken on the recommendation of the Security Commission, to set up a senior security committee on electronic information processing.

RA

ROBERT ARMSTRONG

12 November 1982

Security review ordered on computer files

By Pearce Wright, Science Editor

After allegations in the United States that British computers containing classified information have been penetrated by the Russians, a review of security methods used for computer-stored databanks has been ordered by the Cabinet joint committee on intelligence, which is responsible for all surveillance and counter-espionage at home and abroad.

The review is separate from and not regarded in the same light as the alleged espionage at the General Communications Headquarters at Cheltenham, which has led to reported differences with the Americans.

The concern is about the vulnerability of secret computer files to outsiders using telephone lines and other communication links into the system.

The most obvious protection already recommended is that any computer databank holding top secret files should not form part of one of the growing networks of computers between government and defence departments. The procedure by which any information classified as most confidential then becomes available is by means of a series of personal identity checks.

But the matter of secure communications is crucial for organizations such as oil companies, which transmit information about oil exploration in secret codes, or banks using similar methods to protect commercial data.

Doubts about the need to protect communications should be dispelled by an examination called Cypher Systems, by two experts Dr Henry Beker and Professor Fred Piper, who have developed schemes used by industry and government departments.

They have written a book which describes intercepting secret information as a fascinating battle between code makers and code breakers. They say society is now highly dependent on modern, fast and accurate means of transmitting messages. Usually the main aim is to

send a message as quickly and cheaply as possible. But where the information is confidential and where an interceptor might benefit from monitoring the information circuit, steps to protect communications are needed. On most occasions it is sufficient to prevent a casual "listener" from understanding. The job of preventing the most determined interceptor from monitoring a circuit is more difficult. The best non-interceptible means of transmission is to conceal the content of each message by transforming it before transmission. They say that is the objective of a good cypher system.

Protection and security of communications will grow in the coming years, not only in the traditional military and political fields but also in the public and commercial domain, they say. Their study of cryptography embraces a number of scientific fields, including computer science, electronics, mathematics and statistics.

It is clear that the average cryptographer has a qualification well above the average A level in mathematics.

Their book divides cryptography into a number of stages. First was the simple letter substitution, which could be done with pencil and paper or a simple machine.

The second stage of development dates from the establishment of the telegraph system up to the late 1950s. Those systems, using complicated mechanical and electromechanical machines to provide coding and deciphering methods, were broken by the advent of computers, such as Colossus in Britain, in the Second World War.

The third stage came with advances both in modern mathematics and in the use of microelectronics. Although the complexity of operations now performed by security equipment has risen dramatically, the cost of using sophisticated security devices has fallen.

CONFIDENTIAL



Home Affairs

Lie AH

10 DOWNING STREET

From the Principal Private Secretary

SIR ROBERT ARMSTRONG

SECURITY COMMITTEE ON
ELECTRONIC INFORMATION PROCESSING

The Prime Minister has seen your minute of 11 October (A09692) about the membership of this committee. She is now content that the committee should proceed, with the support outlined in your minute.

F.R.B.

12 October 1982

CONFIDENTIAL

AH



CONFIDENTIAL

Prime Minister

Content that the
Committee should proceed,
with the addition of Mr.
Norman? Background paper
attached. F.R.B.

MR. BUTLER

Yes

Security Committee on Electronic Information Processing

11.10.

Mr. Whitmore's minute of 28th July recorded the Prime Minister's concern about the lack of technical expertise available to this Committee.

2. The new Committee, like its predecessor, is being supported by a number of technical sub-groups whose members have been selected for their knowledge and practical experience in computing and communication security. Many have graduate or post-graduate degrees in Computer Science, Mathematics and Physics. Between them, the members have extensive knowledge and experience in protective and "offensive" security, including such subjects as Cryptography, Electronic Counter-measures and Radio Warfare.

3. This fund of qualifications and experience will be available to the main Committee. In order that the main Committee's resident expertise should be strengthened we have added to it Mr. Adrian Norman, a computer consultant working at present with the Information Technology Unit in the Cabinet Office. Mr. Norman has extensive practical experience of computers, having previously been a systems engineer with IBM and a programme/systems manager for a firm of stockbrokers before becoming a consultant with Interbank Research Organisation and, latterly, a senior management consultant with Arthur D. Little from whom he was seconded to the CPRS in 1980. He is an acknowledged expert on computer frauds, he has published many articles and two books on computer security, and gave evidence to both the Data Protection Committee and the National Committee on Computer Networks.

RIA

Robert Armstrong

11th October 1982

Home Affs, Nov '80, Data Protection



CONFIDENTIAL

NO. 107/80

Handwritten notes in the top left corner, including the word 'Private' and other illegible scribbles.

Main body of the document containing several paragraphs of text, which is extremely faint and mostly illegible due to fading and bleed-through.

CONFIDENTIAL

CONFIDENTIAL



Home Affairs
Jue AH

10 DOWNING STREET

From the Principal Private Secretary

SIR ROBERT ARMSTRONG

SECURITY COMMITTEE ON
ELECTRONIC INFORMATION PROCESSING

I have shown the Prime Minister your minutes A09111 and A09114 of 26 July 1982 about the composition of the Security Committee on Electronic Information Processing.

She has read these papers carefully, including the annex to your minute A09114. Nonetheless, she has minuted as follows:-

"With all due respect, my doubts remain. Unless membership of the British Computer Society requires a high computer qualification, the Committee itself is short on expertise".

Is there any more you can tell the Prime Minister about the qualifications and experience of the members of the Committee which might convince her that the Committee is well equipped to undertake the tasks set in its terms of reference ?

JAW.

28 July 1982

CONFIDENTIAL

AH

MR. WHITMORE

Security Committee on Electronic Information Processing

In the course of preparing herself for supplementaries following the statement on the Prime case, the Prime Minister asked about arrangements for implementing the Security Commission's recommendations for improving the arrangements at official level for dealing with the security risks involved in electronic information processing.

2. A sub-committee of the Official Committee on Security on Electronic Information Processing has been set up under the chairmanship of Mr Colin Peterson, the Under Secretary in the MPO within whose responsibilities security comes. Mr Peterson also chairs the other two sub-committees on security, ie the Personnel Security Committee and the Security Policy and Methods Committee. A list of the departmental representatives nominated by Permanent Secretaries for SCEIP is attached. They are all at about Assistant Secretary level, and have a wide range of background experience covering both physical and communications security and the technological aspects of computing.

3. Other Departments and experts will be invited to attend meetings of the Committee as necessary.

4. The terms of reference of the Committee are as follows:

- i. To keep under review policy and practice for the protection of classified information processed by Automatic Data Processing systems, including office electronic equipment.
- ii. As a secondary concern, to consider the protection of unclassified information similarly processed.
- iii. To maintain close liaison with experts who have a corresponding responsibility for security of electronic information processing in the United States of America.
- iv. To report to the Official Committee on Security any changes required in existing policy, practice and guidance for Departments.
- v. To submit a report annually to the Official Committee on Security.

RA

Robert Armstrong

26th July 1982

SECRET

SECURITY COMMITTEE ON ELECTRONIC INFORMATION PROCESSING (SCEIP)

Departmental representatives

Treasury (CCTA)

Mr B W Smith (Assistant Secretary)

Head of the Computer and Telecommunications Projects Division of CCTA. Is a member of the British Computer Society and his previous experience includes running a hospital computer system at St Thomas' Hospital from 1968-69. Was Chairman of the old SCEIP Committee.

Home Office

Mr W J Cane (Senior Principal)

Currently Head of the Home Office Organisation and Methods Unit with responsibility for the introduction of new technology and related new office equipment. His computer experience goes back to 1966. He was a lecturer in ADP at the Civil Service College from 1974-76. He is a Member of the British Computer Society and holds a certificate as a computer systems analyst issued by the National Computer Centre.

Foreign and Commonwealth Office

Mr A L Barker (Assistant Secretary level)

Head of the FCO Communications and Technical Services Department and has 23 years' experience in dealing with the security aspects of electronic information processing.

Ministry of Defence

Mr M Holton (Assistant Secretary)

Director of Headquarters Security at MOD. Responsible for all aspects of both personnel and physical security and is a member of the Security Policy and Methods Committee.

Government Communications Headquarters

THIS IS A COPY. THE ORIGINAL IS
RETAINED UNDER SECTION 3 (4)
OF THE PUBLIC RECORDS ACT

Security Service

Communications Electronics Security Group

THIS IS A COPY. THE ORIGINAL IS
RETAINED UNDER SECTION 3 (4)
OF THE PUBLIC RECORDS ACT

Prime Minister.

*With all due respect -
my shoulder remains
Under membership of the
Advisory Committee - Security
reference - high
computer technology
the committee
is expected*

*There is a note later too
you should see it
short*

Ref. A09111

MR WHITMORE

I attach a note about the composition of the new Security Committee on Electronic Information Processing.

2. When we were discussing the Prime Minister's statement last week, she expressed doubt - if that is not too mild a word - whether Mr Peterson was suitably qualified to be the Chairman of this Committee.

3. Of course he is new to security matters, as to other things in the MPO for which he now has some responsibility. But he is intelligent, conscientious and well-supported, and he is as capable as any one of making himself the master of the subject in general.

4. A committee on computer security will require, in addition to expertise on security, expertise on computers. That is well catered for in the list of members of the new Committee, attached to my minute. With respect, I do not think that it is necessary for the Chairman to be an expert in computers. Indeed the Security Commission said that one of the difficulties was that the existing instructions on computer security were so technical that they might not be readily understood by security officers in Departments who would be called upon to apply them. There will be much to be said for having a Chairman who will have available to him the advice which will enable him to ensure that the instructions are technically correct and will also have the skill to ensure that they are clear and comprehensible to those whose technical knowledge may be limited.

RA

ROBERT ARMSTRONG

26 July 1982

PRIME MINISTER

H Committee Minutes

You will already have seen the Home Secretary's paper on data protection which was discussed by the H Committee meeting on 7 July. As you will see, subject to a number of relatively minor points together with the major fear that the right of access to data would impose manpower burdens on some departments, the Home Secretary's proposals were agreed. The Committee however were in no doubts that legislation would be contentious and proposed therefore that the Data Protection Bill should, subject to discussion in Legislation Committee, be ready as early as possible in the 1982/3 Session and should be introduced in the House of Lords.

8 July 1982

PRIME MINISTER

DATA PROTECTION

You may be interested to see the attached note of a consideration by H Committee on the bill embodying the Government's proposals on data protection. The main points are:-

- (1) the establishment of a data protection registrar, independent of government;
- (2) the requirement that all users of automatically processed personal data should register;
- (3) that the only exemptions should be for small-scale or domestic use or for sensitive, or law enforcement use. Exemptions are to be ratified by ministerial certificate;
- (4) the absence of any general legal requirements in data users; the sanction for inappropriate use will be the registrar's power to refuse registration;
- (5) provision for access by subjects to data held on them (other than in exempt cases) on payment of a fee;
- (6) funding of the registrar to be by grant and aid, recoverable through fees charged to users.

TF

30 June 1982

From: THE PRIVATE SECRETARY

✓ MAP
Press Office



Prime Minister 4

HOME OFFICE
QUEEN ANNE'S GATE
LONDON SW1H 9AT

To be aware that
the Home Office proposes to publish
this White Paper next
Wednesday.

WR 31/3 31 MAR 1962

mt

DATA PROTECTION

I wrote to you on 19th March enclosing a draft White Paper. You kindly let me have comments on it in your letter of 26th March, as did the Northern Ireland Office, the Department of Trade, the Treasury, the Welsh Office, and the Department of Industry.

... We have taken those comments into account in the enclosed redraft, which we are now sending to the Printers. We are aiming for publication on 7th April.

Copies of this letter and enclosure go to the Private Secretaries to the Prime Minister, other members of Cabinet and to David Wright (Cabinet Office).

A. P. JACKSON

Brendan O'Gorman, Esq.



HOME OFFICE

~~DATA PROTECTION~~

The Government's Proposals for Legislation

*Presented to Parliament by the Secretary of State for the Home Department,
by Command of Her Majesty
April 1982*

LONDON

HER MAJESTY'S STATIONERY OFFICE

£. net

Cmnd. 227

Copy sent to ...

B.R.

DATA PROTECTION

The Government's intention to introduce legislation on data protection was announced in the Home Secretary's statement of 19 March 1981. The object of this White Paper is to explain the proposals and the background to them in more detail.

Background to the Government's proposals

2. There are two main reasons why legislation is needed. First, because of the threat to privacy posed by ~~the~~ rapid growth in the use of computers, with their ability to process and link at high speed information about individuals. There have been few reported instances in this country of information held on computers being misused so as to threaten the personal privacy of individuals. But the ease and scale of misuse which the versatility of computers makes possible is significantly greater than with manual records. Secondly, without legislation firms operating in the United Kingdom may be at a disadvantage compared with those based in countries which have data protection legislation. When the Council of Europe Data Protection Convention comes into force it will confirm the right of countries with data protection legislation to refuse to allow personal information to be sent to other countries which do not have comparable safeguards. This could threaten firms with international interests operating in this country and the activities of British computer bureaux which increasingly process data for customers in many different countries. Accordingly, in order to conform with international standards of privacy protection and to avoid possible barriers to trade, the Government has decided to introduce legislation which will apply throughout the United Kingdom and will enable the United Kingdom to ratify the Convention. The legislation will be designed to impose no greater burden on our resources than is necessary.

3. The Younger Committee on Privacy was appointed by the Government of the day in May 1970 and reported in 1972. It set out certain principles in regard to computer privacy which were intended as general guidelines to computer users in the private sector. The Government believes that with suitable adaptation, and taking account of the text of the Convention, these

principles form a starting point for enforceable rules of law applying to both the private and the public sectors.

4. In 1975 the Government of the day announced in a White Paper ("Computers and Privacy", Cmnd 6353 and its supplement, "Computers: Safeguards for Privacy", Cmnd 6354) its decision to prepare legislation setting out the standards governing the use of computers that process personal information and establishing a statutory data protection authority to oversee the use of computers with regard to privacy. A Data Protection Committee under the chairmanship of Sir Norman Lindop was appointed to advise on the legislation. The Lindop Committee reported in 1978 (Cmnd 7341). The report contains very helpful background information and a valuable analysis of ways of overcoming the problems involved.

5. In the meantime the Council of Europe has prepared a Convention on Data Protection* which was opened for signature in January 1981 and was signed by the United Kingdom in May of that year. In addition the Organisation for Economic Co-operation and Development has prepared guidelines on privacy protection and transborder data flows which the United Kingdom endorsed in September 1981. The Convention and the Guidelines are reproduced as Annexes A and B to this White Paper. Eight European States (Austria, France, Denmark, Iceland, Luxembourg, Norway, Sweden and the Federal Republic of Germany) now have data protection legislation in force, and others (including Finland, the Netherlands and Switzerland) are about to introduce legislative proposals. Eleven States (Austria, Denmark, France, Luxembourg, Norway, Sweden, Turkey, the Federal Republic of Germany, Portugal, the United Kingdom and Spain) have signed the Council of Europe Convention, but none has yet ratified it, and the Convention has not yet entered into force. It will do so when five States have ratified it.

The general principles

6. The general principles set out in the Younger Report (see para 3 above) were broadly endorsed by the Lindop Committee and have been embodied in the Data Protection Convention. The principles (following Articles 5, 7 and 8 of the Convention) are as follows:

- E.R.
- (i) The information shall be obtained and processed fairly and lawfully;
 - (ii) It shall be held for a specified and legitimate purpose or purposes;
 - (iii) It shall not be used or disclosed in a way incompatible with those purposes;
 - (iv) It shall be adequate, relevant, and not excessive in relation to the specified purposes;
 - (v) It shall be accurate and, where necessary, kept up to date;
 - (vi) It shall be kept in name linked form for no longer than is necessary for the specified purposes;
 - (vii) The data subject shall have access to information held about him and be entitled to its correction or erasure where the legal provisions safeguarding personal data have not been complied with.
 - (viii) Appropriate security measures must be taken against unauthorised access, alteration or dissemination, accidental loss and accidental or unauthorised destruction of data.

7. The Government proposes that these principles should be embodied in the legislation. The sanctions provided by the legislation (see paragraph 19 below) will be designed to ensure so far as possible, and subject to any exemptions permitted by the legislation and by regulations made under it, that data users comply with the principles. The term 'data user' includes those who collect data, collate or otherwise process data by automatic means, and disseminate data

8. The Lindop Committee recommended that the Data Protection Authority should produce codes of practice which would be laid before Parliament and have the force of law. Some 50 or more codes would apply the general principles to the wide variety of situations in which personal data are

processed automatically. The Government sees some value of codes of practice in this field and expects that some professional bodies, trade associations and other organisations may wish to prepare such codes as a guide to their members. But the Government does not consider that these codes should have the force of law or that it would be practicable, without imposing an unacceptable burden on resources, to cover the whole field of personal data systems with statutory codes of practice within any reasonable timescale. The Government accepts, however, that in some areas (see para 14 below) the general principles will need to be supplemented by regulations.

The Registrar

9. The central feature of the Government's proposals will be a requirement that - with the possible exception of small scale users who keep data for domestic purposes - all users of data systems which process automatically information relating to identifiable individuals should register. The Lindop Committee found that registration schemes were a common feature of data protection legislation in other countries. A public register should go a long way to meet the objective that the existence and purpose of computerised personal information systems should be publicly known. The requirements for registration will be as simple as possible. The data user will normally be required to provide brief particulars identifying him, the information he uses, where it has come from and to whom it is disclosed, and the purposes for which it is used. He will also be required to register any changes in these particulars. It is expected that most applicants will be registered without question but the Registrar will have power to make enquiries, to inspect data files and to require modifications to a system. In extreme cases he may need to refuse registration on the ground that the applicants arrangements do not comply with the general principles. He will also be empowered if the case warrants it, to strike a data user off the register, and to take proceedings against data users (see paragraph 19 below).

10. The Registrar will be appointed by the Crown, and it is proposed that he should serve for five years in the first instance. He will be required to make an annual report to Parliament. He and his staff will be independent

E.R.

of the Government, but the Government will designate him as the authority for rendering assistance to other Parties to the Council of Europe Convention.

11. Initially the Registrar may need a staff of about 20 (who should include computer experts) to set up the register as soon as possible after the legislation comes into force. While he will not have the resources to supervise the operation of data systems in detail, he will be expected to offer advice to data users and data subjects; to follow up cases where defects are/ ^{identified} at the point of registration, to pursue complaints and give guidance on codes of practice.

Appeal Tribunal

12. The Registrar will have wide powers and it will be appropriate for there to be a right of appeal against his decisions. It is proposed that this should lie to an independent tribunal under a legally qualified chairman appointed by the Lord Chancellor. The members of the tribunal would be drawn from a panel which would include computer experts.

The Public Sector

13. Subject to the exemptions allowed in the legislation (see paragraph 17 below), central Government, local authorities, the police, nationalised industries and other public sector bodies will be required to register in the same way as other users. The register will clearly indicate the purposes for which these bodies use data relating to individuals and any arrangements for transferring such data from one organisation to another.

Special cases and exemptions

14. The power to make regulations (see para 8 above) will be needed to deal, amongst other things, with the processing of categories of data where it is not sufficient to rely on the general principles alone and where Parliament may expect to see detailed requirements laid down. Thus the Convention prohibits the processing of data revealing racial origin, political opinions or religious or other beliefs, health or sexual life

and criminal convictions unless the law provides appropriate safeguards. Some of these categories of data (and in particular medical records) may well need to be covered by regulations which might, for example, place special restrictions on the collection, processing, holding or disclosure of information from such records.

15. The collection and use of data solely for statistical or research purposes do not threaten the privacy of data subjects, provided that in processing and disseminating the results steps are taken against revealing information about an identifiable individual. For this reason, the principle that the data subject should have access to information held about him need not apply to records held solely for these purposes, nor need the information be absolutely accurate and up to date. This should apply equally to data specially collected for a statistical or research purpose and to data originally collected for administrative or other purposes.

16. The collection of information for the purposes of public records and other archives is already governed by specific legislation. It is not intended that the data protection legislation should inhibit the preservation of historically valuable data for these purposes.

17. The Convention permits derogation from the general principles (except in relation to measures to ensure the security of systems) in the interests of:

- "a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
- b. protecting the data subject or the rights and freedoms of others."

In accordance with the provisions at a. above it is proposed that the legislation should not apply to data that need to be safeguarded for the purposes of national security. The use of certain other data relating to the matters referred to at a. above will be exempt from registration.

These exemptions will include some data needed by the police and other law enforcement agencies for the prevention and detection of crime. But the intention will be to keep exemptions from registration to the minimum that is consistent with the proper functioning of the agencies^{concerned}. Similarly, registered data users who make information available to the authorities in connection with these matters will not be required to register such disclosures of information. To register them would tend to defeat the purpose for which they are made. The provisions at b. above are likely to apply in the case of medical records and possibly in certain other areas such as sensitive information recorded by social workers. In such cases - as for some within the scope of (a) - the user will have to be registered but it may be appropriate to restrict access by the data subject.

18. Those who use computer bureaux will have to register, as will the bureaux themselves. The latter will, however, be exempt from compliance with some of the general principles because it is not normally the bureau but the user who controls the purpose, collection, dissemination, and access to the data.

Sanctions

19. Criminal and civil sanctions will be tailored to fit the general principles of the scheme and to complement the powers given to the Registrar. It is proposed to make it an offence to make a false statement to the Registrar; to process personal information automatically without being registered or exempted from registration; or to fail to comply with a notice served by the Registrar regarding a defect to be remedied. For the most part the general principles are not expressed in language which would make it appropriate for their breach to constitute a criminal offence. But it is for consideration whether provision should be made for criminal sanctions where a data user deliberately records, uses or disseminates false information, refuses access to a data subject without good cause, or uses information for a purpose which is not registered.

20. The main purpose of the civil remedies will be to ensure that data subjects who have suffered damage because of a breach of the requirements governing data use can secure compensation, although injunctions will be

available to restrain breaches of a statutory requirement where damage is anticipated but has not yet been suffered. It is not envisaged that the Registrar will have any role to play in relation to civil proceedings, which will be the responsibility of the individual who alleges he has suffered damage. It is for consideration what form the liability should take. Liability dependent upon proof of fault would present difficulties for the plaintiff who would not often be in a position to adduce detailed technical evidence about the data user's operations. From the point of view of the plaintiff, some form of strict liability would be most effective. The form is again open for consideration: for instance, whether statutory defences might be available to the user, allowing him to avoid or limit liability where he had done all that was reasonable in the circumstances or could, perhaps, establish that he had not been at fault.

21. Whether or not there appears to be a breach of data protection legislation, complaints about public sector data systems which allege injustice caused by maladministration may also fall to be investigated under the relevant legislation by the Parliamentary Commissioner for Administration or where appropriate the Northern Ireland Parliamentary Commissioner for Administration. Where relevant legislation applies complaints may also be taken up with the Health Services Commissioners or the Commissioner for local Administration as the case may be. Similarly, complaints relating to the health service or various local services in Northern Ireland may be investigated by the Northern Ireland Commissioner for Complaints.

Transfer of data to other countries

22. The legislation will enable the Government to restrict the transfer of categories of information to specified countries whose laws do not provide comparable safeguards for the privacy of computerised personal information in the categories concerned.

Costs

23. In accordance with the Government's objective of keeping the burden on resources to a minimum, everything possible will be done to ensure that neither the legislation nor the regulations made under it impose unnecessarily costly requirements. In the public sector costs and manpower will have to be contained within existing planned totals, even if this means deferring

application of the legislation in some areas. The initial cost of the Registrar and his staff (see para 11 above) is likely to be of the order of £500,000 a year at 1981/82 prices. It is the intention that the fees charged by the Register will recover all his costs, including those of setting up the register. Every effort will be made to keep costs down, and the registration fees will represent only a minute proportion of the total cost of a data system.

24. Where a data subject is granted access to information relating to him he will normally be expected to pay a fee. The access fee is a common feature of all European schemes. Charges made to data subjects generally on access to information should be based on the principle that the costs for the demands are fully recovered.

25. An effective data protection system, however simple, is going to mean that some users incur increased capital costs for developing their hardware or software systems, and increased running costs as a result of responding to requests for access. But these implementation costs have to be balanced against the potential benefits. In particular data protection legislation is needed to ensure that the United Kingdom's substantial international trade in information, and its key role as a crossroads on the international data highway, are not compromised.

Timing of implementation

26. The registration process will take a considerable time. ^{perhaps 2 years} Moreover users of particular categories of data may not be able, for financial or other reasons (see paragraph 23 above) to meet the full requirements of the legislation until some time after registration. The European Convention allows for phased implementation of data protection arrangements.

An Advisory Committee

27. Once the legislation is in force it might be appropriate to appoint an Advisory Committee to advise the Government on the preparation of

regulations relating to particular categories of data and, if the need arose, on possible changes to the legislation itself.

Conclusion

28. The Government believes that the proposals in this White Paper will safeguard privacy, protect our trading interests and enable the United Kingdom to ratify the Council of Europe Convention, and intends to legislate on these lines.

29. Any comments on these proposals should be sent by 31st May 1982 to the Home Office, E1 Division, Room 814, Queen Anne's Gate, London, SW1.

COUNCIL OF EUROPE

CONVENTION FOR THE PROTECTION OF INDIVIDUALS
WITH REGARD TO AUTOMATIC PROCESSING
OF PERSONAL DATA

PREAMBLE

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms ;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing ;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers ;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows :

CHAPTER I — GENERAL PROVISIONS

Article 1

Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2

Definitions

For the purposes of this convention :

- a. "personal data" means any information relating to an identified or identifiable individual ("data subject") ;
- b. "automated data file" means any set of data undergoing automatic processing ;
- c. "automatic processing" includes the following operations if carried out in whole or in part by automated means : storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination ;
- d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3

Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe :

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law ;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality ;

c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.*b* or *c* above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.*a* above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.*b* and *c* above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II — BASIC PRINCIPLES FOR DATA PROTECTION

Article 4

Duties of the Parties

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

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

Article 5
Quality of data

Personal data undergoing automatic processing shall be :

- a. obtained and processed fairly and lawfully ;
- b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes ;
- c. adequate, relevant and not excessive in relation to the purposes for which they are stored ;
- d. accurate and, where necessary, kept up to date ;
- e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6
Special categories of data

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

Article 7
Data security

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

Article 8
Additional safeguards for the data subject

Any person shall be enabled :

- a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file ;
- b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form ;
- c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention ;
- d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9
Exceptions and restrictions

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

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

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

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

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

Article 10

Sanctions and remedies

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

Article 11

Extended protection

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

CHAPTER III — TRANSBORDER DATA FLOWS

Article 12

Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2 :

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection ;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

CHAPTER IV — MUTUAL ASSISTANCE

Article 13

Co-operation between Parties

1. The Parties agree to render each other mutual assistance in order to implement this convention.
2. For that purpose :
 - a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe ;
 - b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.
3. An authority designated by a Party shall at the request of an authority designated by another Party :
 - a. furnish information on its law and administrative practice in the field of data protection ;
 - b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14

Assistance to data subjects resident abroad

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.
2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.
3. The request for assistance shall contain all the necessary particulars, relating *inter alia* to :
 - a. the name, address and any other relevant particulars identifying the person making the request ;
 - b. the automated personal data file to which the request pertains, or its controller ;
 - c. the purpose of the request.

Article 15

Safeguards concerning assistance rendered by designated authorities

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.
2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3. In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16

Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless :

- a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying ;
- b. the request does not comply with the provisions of this convention ;
- c. compliance with the request would be incompatible with the sovereignty, security or public policy (*ordre public*) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17

Costs and procedures of assistance

1. Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.
2. The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.
3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

CHAPTER V — CONSULTATIVE COMMITTEE

Article 18

Composition of the committee

1. A Consultative Committee shall be set up after the entry into force of this convention.
2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.
3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19

Functions of the committee

The Consultative Committee :

- a. may make proposals with a view to facilitating or improving the application of the convention ;

b. may make proposals for amendment of this convention in accordance with Article 21 ;

c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3 ;

d. may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20

Procedure

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.
2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.
3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.
4. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

CHAPTER VI — AMENDMENTS

Article 21

Amendments

1. Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.
2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.
3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.
4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.
5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.
6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII — FINAL CLAUSES

Article 22

Entry into force

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.
3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23

Accession by non-member States

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.
2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24

Territorial clause

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.
2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.
3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25

Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26

Denunciation

1. Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.
2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27

Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of :

- a. any signature ;
- b. the deposit of any instrument of ratification, acceptance, approval or accession ;
- c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24 ;
- d. any other act, notification or communication relating to this convention.

RECOMMENDATION OF THE COUNCIL OF THE OECD
CONCERNING GUIDELINES GOVERNING THE PROTECTION OF
PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

The Council,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

Recognising:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof:

(*) The Australian, Canadian, Icelandic, Irish, Turkish and United Kingdom Governments abstained.

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY
AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:
 - (a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
 - (b) "personal data" means any information relating to an identified or identifiable individual (data subject);
 - (c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.
3. These Guidelines should not be interpreted as preventing:
 - (a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
 - (b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
 - (c) the application of the Guidelines only to automatic processing of personal data.
4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- (a) as few as possible, and
 - (b) made known to the public.
5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.
6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject:

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
- (a) with the consent of the data subject; or
 - (b) by the authority of law.

Security Safeguards Principle

- 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

- 12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

- 13. An individual should have the right:
 - (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
 - (b) to have communicated to him, data relating to him
 - (i) within a reasonable time;
 - (ii) at a charge, if any, that is not excessive;
 - (iii) in a reasonable manner; and
 - (iv) in a form that is readily intelligible to him;
 - (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
 - (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

- 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION:
FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:
 - (a) adopt appropriate domestic legislation;
 - (b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
 - (c) provide for reasonable means for individuals to exercise their rights;

- (d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- (e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

- 21. Member countries should establish procedures to facilitate:
 - (i) information exchange related to these Guidelines, and
 - (ii) mutual assistance in the procedural and investigative matters involved.
- 22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.



Home Affairs
WR
29/3

Treasury Chambers, Parliament Street, SW1P 3AG

A P Jackson Esq
Private Secretary to
Rt Hon William Whitelaw CH MC MP
Secretary of State
Home Office
50 Queen Anne's Gate
London SW1H 9AT

29 March 1982

Dear Andrew,

DATA PROTECTION WHITE PAPER

Thank you for sending us a copy of your letter of 19 March inviting comments on the draft White Paper on data protection legislation.

We have a couple of points which we should like to see taken in the draft. The first concerns the position of the Revenue Departments. Paragraph 17 seems to have been written almost entirely from the viewpoint of national security and law enforcement agencies. That is, of course, understandable. But there are clear cut cases where in "the monetary interests of the State" both the Customs and Excise and the Inland Revenue will store data of valuable criminal intelligence use that goes wider than revenue evasion. To take these points the fourth sentence of paragraph 17 (at the top of page 7) should be amended to read:

"These exemptions will include, for example, some data needed by the police and analogous law enforcement bodies for the prevention and detection of crime."

And the fourth sentence on this page should finish as follows:-

".... the minimum that is consistent with the proper functioning of the enforcement agencies concerned."

Your approach to cases in (a) in paragraph 17 deals with the concept of exemption from registration. In certain cases it might be appropriate to register a system but to impose

restrictions on access. This could certainly be feasible for the Inland Revenue, and for other applications. This alternative should be made clear, particularly as it affects both the rights of the State and those of the data subject. The point would be met if the final sentence of paragraph 17 was amended to read:-

"In such cases - as for some within (a) - the user will have to be registered, but it may be appropriate to restrict access by the data subject."

The second comment concerns the recovery of certain costs by fees. Our discussions have been based on the concept of full cost recovery, both for fees set by the Registrar and those charged by data users on data subjects. The policy on the former is clearly set out in paragraph 23. But paragraph 24 is unsatisfactory because it implies that a different principle may apply in the case of charges to data subjects. We should not want such a hostage to fortune in the White Paper, as it runs contrary to general policy. Recognising that in some instances there may be initial capital costs which could not reasonably be charged to a small number of initial users, we suggest that the first sentence of paragraph 24 (which might become the final sentence of paragraph 23) could read as follows:-

"Charges made to data subjects generally on access to information should be based on the principle that the costs of the demands they make are fully recovered."

- Because of the implication it carries that fees might be subsidised we should prefer the final sentence of paragraph 24 to be deleted. This applies also, we think, to the second part of the first sentence in paragraph 25.

Finally, we should like to comment on the potential conflict between statements in paragraph 23 and paragraph 26. Paragraph 23 properly says that it may be necessary to defer application of the system in the public sector if this cannot be contained within existing planned totals. However, paragraph 26 suggests that the register should be fully operative within two years. I understand that officials have agreed that the next sentence of paragraph 26 ('a longer period may be necessary') may not adequately qualify the suggestion that 'up to two years' may be needed, and that the latter needs to be amended.

I am sending copies of this letter to the Private Secretaries to the Prime Minister, other members of the Cabinet, the Chief Whips (Lords and Commons) and to Sir Robert Armstrong.

Yours sincerely

Terry Matthews

T F MATHEWS
Private Secretary



DEPARTMENT OF HEALTH AND SOCIAL SECURITY
 ALEXANDER FLEMING HOUSE
 ELEPHANT AND CASTLE LONDON SE1 6BY
 TELEPHONE 01-407 5522 EXT

Andrew Jackson Esq
 Private Secretary to
 Secretary of State for the Home Department
 Home Office
 50 Queen Anne's Gate
 London SW1

26 March 1982

Prime Minister 2

Dear Andrew

*Some markers from Mr Parker on the
 cost of making official information
 available to the public.*

DATA PROTECTION

You sent me a copy of the latest draft of the White Paper on 19 March. My Secretary of State agrees that publication should now go ahead quickly and has no comments on the content of the draft White Paper itself. There are however one or two general points which he thinks it would be useful to make at this stage on the effects of publication of the White Paper.

There is the question of the manpower needed if a significant number of people seek to be informed about the content of their records. As you will realise, there is a social security record of one sort or another for virtually every person in the country. It is very difficult to estimate the percentage of those people who would seek details of the information we are holding and comparison of estimates from other countries may not prove to be a reliable basis. However, if even one per cent sought details of those records we would need on present estimates some 350 extra staff. Even if, by charging for provision of the information, the scheme could be made self-financing it would nevertheless affect the headcount of staff and the total number of civil servants would inevitably increase. In this connection we already give national insurance contributors details of their record, free of charge, if they ask for it. We do not think it would be appropriate to charge for this - some people need the details in order to plan their future - on the other hand we would not want legislation in another field to encourage frivolous or unnecessary applications. These points are made now by way of markers on items which will need to be watched when legislation comes to be drafted.

One final small presentational point is that it seems odd to ask for comments in a footnote. If comments are to be sought - even though this is a White Paper - it would seem best to do so in a final paragraph to the conclusion as in an earlier draft; this is after all a matter of considerable political interest.

I am copying this letter to the recipients of yours.

*yours ever,
 Brendan*

BRENDAN O'GORMAN
 Private Secretary

LM 2/13
3 pp's.

From the Secretary of State

A P Jackson Esq
Private Secretary to the
Home Secretary
Home Office
Queen Anne's Gate
London SW1H 9AT

26th March 1982

Dear Andrew,

DATA PROTECTION

Your letter of 19 March to Brendon O'Gorman invited comments on the draft White Paper the Home Secretary had asked to be circulated. My Secretary of State is broadly content but has asked for a number of points to be considered.

The first, which is certainly of substance, occurs at paragraph 7 of the draft. Surely the point of the legislation, and of regulations made under it, will be to 'require' data users to comply with the principles. My Secretary of State fears that the use of the word 'expected' in this critical passage in the draft will give the wrong impression of the discipline which is intended, both to commercial interests at home and authorities overseas. After all, an important objective of this legislation is to ensure that data in the UK is regarded as sufficiently well protected for overseas interests to be free to send it here for processing.

Next, also with some bearing on the impression the draft conveys about the nature of the scheme being proposed, we think third sentence of paragraph 8 would give a better impression of the distance of what is intended from Lindop Codes of Practice and concomitant machinery, if it were to read 'The Government sees some value in codes of practice in this field and expects that some professional bodies, trade associations and other organisations may wish to prepare such codes as a guide to their members.'

5-2-1982



From the Secretary of State

In the same vein, paragraph 9 reads as though the Registrar will closely peruse the detail of all registration documents, and it gives no indication, as my Secretary of State believes is intended, that registration per se will not imply that the Registrar is content that a system being registered actually complies with the principles. To this end he suggests the words 'capable of registration' should replace 'registered' at line 10, and that a disclaimer about the Registrar's accepting registration should be inserted towards the end of the paragraph, perhaps by adding the words ', but the fact that he accepts a set of particulars for registration will not mean that he is satisfied the system being registered necessarily meets the principles.' to the penultimate sentence as presented drafted.

A further point that concerns my Secretary of State is that paragraph 22 on the transfer of data to other countries makes no mention of the Government's thinking on who will exercise power to restrict transfer, or what, if any, appeal there may be. This, he thinks, will be a matter of some concern to commercial interests, and he would see advantage if thinking on the matter could be indicated. His view is that power should be vested in a Secretary of State, advised by the Registrar.

Finally, he has questioned the inclusion of the phrase 'designed to offset the costs of access' in the first sentence of paragraph 24, which is about fees. The phrase lies oddly with the remainder of the paragraph, and with the reference to some users incurring increased running costs as a result of responding to requests for access in the following paragraph.

Subject to these points, my Secretary of State will be glad to see the White Paper published as quickly as possible, as you record the Home Secretary intends.

I am copying this letter to Private Secretaries to the Prime Minister, other members of the Cabinet, Chief Whips (Lords and Commons) and to Sir Robert Armstrong.

Yours Sincerely,
Jonathan Rees

JONATHAN REES
Private Secretary

29 MAR 1982

WR 1/3



Y SWYDDFA GYMREIG
GWYDYR HOUSE
WHITEHALL LONDON SW1A 2ER
Tel. 01-233 3000 (Switsfwrdd)
01-233 8545 (Llinell Union)

ODDI WRTH YSGRIFENNYDD
PREIFAT YSGRIFENNYDD
GWLADOL CYMRU

WELSH OFFICE
GWYDYR HOUSE
WHITEHALL LONDON SW1A 2ER
Tel. 01-233 3000 (Switchboard)
01-233 8545 (Direct Line)

FROM THE PRIVATE SECRETARY
TO THE SECRETARY OF STATE
FOR WALES



26 March 1982

Dear Andrew

DATA PROTECTION

Thank you for your letter of 19 March enclosing the draft White Paper on Data Protection.

My Secretary of State is content with the draft and agrees that the White Paper should be published as soon as possible.

/ I am copying this letter to the recipients of yours.

Yours ever
J F Craig
J F CRAIG
Private Secretary

A P Jackson Esq
Home Office
Queen Anne's Gate
LONDON SW1H 9AT

Home Affairs



NORTHERN IRELAND OFFICE
GREAT GEORGE STREET,
LONDON SW1P 3AJ

WM 25/3

A P Jackson Esq
Private Secretary to
the Home Secretary
Home Office
Queen Anne's Gate
LONDON
SW1H 9AT

25 March 1982

Dear Andrew,

DATA PROTECTION

Thank you for sending me a copy of your letter of 19 March to Brendon O'Gorman to which you attached a copy of the draft White Paper on data protection legislation.

I understand that in further discussions between officials it has been agreed that in order to distinguish more clearly between the jurisdictions of the various 'ombudsmen' mentioned in paragraph 21 it would be helpful if that paragraph could be revised to read as follows:

"Whether or not there appears to be a breach of data protection legislation, complaints about public sector data systems which allege injustice caused by maladministration may also fall to be investigated under the relevant legislation by the Parliamentary Commissioner for Administration or where appropriate the Northern Ireland Parliamentary Commissioner for Administration. Where relevant legislation applies complaints may also be taken up with the Health Services Commissioners or the Commissioner for Local Administration as the case may be. Similarly, complaints relating to the health service or various local services in Northern Ireland may be investigated by the Northern Ireland Commissioner for Complaints".

Subject to this revision being incorporated in the final revise we are content with the draft.

I am copying this letter to Private Secretaries to the Prime Minister and other members of the Cabinet, and to David Wright (Cabinet Office).

Yours sincerely
M W Hopkins

M W HOPKINS

From: THE PRIVATE SECRETARY

Note: I have told the Home Office that the pm is content. WH 22/3

Home Affairs

HOME OFFICE
QUEEN ANNE'S GATE
LONDON SW1H 9AT



19 March 1982

Dear Brendan

Yes
out

Prime Minister cc my Ingham

DATA PROTECTION

This follows the lines of the H Paper on data protection which you saw in February. Content?

WH
19/3

H Committee on 23 February approved proposals for a White Paper on data protection legislation. I now enclose a draft White Paper which follows the lines of the paper considered at H Committee and has been discussed at official level by the Departments concerned.

The Home Secretary thinks it is important that we should publish the White Paper as soon as possible, so as to allow time for public reaction to our proposals before legislation is prepared. If your Secretary of State or any colleagues have any comments on the enclosed draft we should be glad to have them by not later than 26 March.

I am copying this letter and enclosure to Private Secretaries to the Prime Minister, other members of the Cabinet, Chief Whips (Lords and Commons) and to Sir Robert Armstrong.

Yours ever
A P Jackson

A P JACKSON

Brendon O'Gorman, Esq.

DRAFT WHITE PAPER 11/3/82

DATA PROTECTION

The Government's intention to introduce legislation on data protection was announced in the Home Secretary's statement of 19 March 1981. The object of this White Paper is to explain the proposals and the background to them in more detail.

Background to the Government's proposals

2. There are two main reasons why legislation is needed. First, because of the threat to privacy posed by the rapid growth in the use of computers, with their ability to process and link at high speed information about individuals. There have been few reported instances in this country of information held on computers being misused so as to threaten the personal privacy of individuals. But the ease and scale of misuse which the versatility of computers makes possible is significantly greater than with manual records. Secondly, without legislation firms operating in the United Kingdom may be at a disadvantage compared with those based in countries which have data protection legislation. When the Council of Europe Data Protection Convention comes into force it will confirm the right of countries with data protection legislation to refuse to allow personal information to be sent to other countries which do not have comparable safeguards. This could threaten firms with international interests operating in this country and the activities of British computer bureaux which increasingly process data for customers in many different countries. Accordingly, in order to conform with international standards of privacy protection and to avoid possible barriers to trade, the Government has decided to introduce legislation which will apply throughout the United Kingdom and will enable the United Kingdom to ratify the Convention. The legislation will be designed to impose no greater burden on our resources than is necessary.

3. The Younger Committee on Privacy was appointed by the Government of the day in May 1970 and reported in 1972. It set out certain principles in regard to computer privacy which were intended as general guidelines to computer users in the private sector. The Government believes that with suitable adaptation, and taking account of the text of the Convention, these

principles form a starting point for enforceable rules of law applying to both the private and the public sectors.

4. In 1975 the Government of the day announced in a White Paper ("Computers and Privacy", Cmnd 6353 and its supplement, "Computers: Safeguards for Privacy", Cmnd 6354) its decision to prepare legislation setting out the standards governing the use of computers that process personal information and establishing a statutory data protection authority to oversee the use of computers with regard to privacy. A Data Protection Committee under the chairmanship of Sir Norman Lindop was appointed to advise on the legislation. The Lindop Committee reported in 1978 (Cmnd 7341). The report contains very helpful background information and a valuable analysis of ways of overcoming the problems involved.

5. In the meantime the Council of Europe has prepared a Convention on Data Protection* which was opened for signature in January 1981 and was signed by the United Kingdom in May of that year. In addition the Organisation for Economic Co-operation and Development has prepared guidelines on privacy protection and transborder data flows which the United Kingdom endorsed in September 1981. The Convention and the Guidelines are reproduced as Annexes A and B to this White Paper. Eight European States (Austria, France, Denmark, Iceland, Luxembourg, Norway, Sweden and the Federal Republic of Germany) now have data protection legislation in force, and others (including Finland, the Netherlands and Switzerland) are about to introduce legislative proposals. Eleven States (Austria, Denmark, France, Luxembourg, Norway, Sweden, Turkey, the Federal Republic of Germany, Portugal, the United Kingdom and Spain) have signed the Council of Europe Convention, but none has yet ratified it, and the Convention has not yet entered into force. It will do so when five States have ratified it.

The general principles

6. The general principles set out in the Younger Report (see para 3 above) were broadly endorsed by the Lindop Committee and have been embodied in the Data Protection Convention. The principles (following Articles 5, 7 and 8 of the Convention) are as follows:

- (i) The information shall be obtained and processed fairly and lawfully;
- (ii) It shall be held for a specified and legitimate purpose or purposes;
- (iii) It shall not be used or disclosed in a way incompatible with those purposes;
- (iv) It shall be adequate, relevant, and not excessive in relation to the specified purposes;
- (v) It shall be accurate and, where necessary, kept up to date;
- (vi) It shall be kept in name linked form for no longer than is necessary for the specified purposes;
- (vii) The data subject shall have access to information held about him and be entitled to its correction or erasure where the legal provisions safeguarding personal data have not been complied with.
- (viii) Appropriate security measures must be taken against unauthorised access, alteration or dissemination, accidental loss and accidental or unauthorised destruction of data.

7. The Government proposes that these principles should be embodied in the legislation. Subject to any exemptions permitted by the legislation or by regulations made under it, data users will be expected to comply with the principles. The term 'data user' includes those who collect data, collate or otherwise process data by automatic means, and disseminate data.

8. The Lindop Committee recommended that the Data Protection Authority should produce codes of practice which would be laid before Parliament and have the force of law. Some 50 or more codes would apply the general principles to the wide variety of situations in which personal data are

processed automatically. The Government sees the value of codes of practice in this field and expects that some professional bodies, trade associations and other organisations will wish to prepare such codes as a guide to their members. But the Government does not consider that these codes should have the force of law or that it would be practicable, without imposing an unacceptable burden on resources, to cover the whole field of personal data systems with statutory codes of practice within any reasonable timescale. The Government accepts, however, that in some areas (see para 14 below) the general principles will need to be supplemented by regulations.

The Registrar

9. The central feature of the Government's proposals will be a requirement that all users of data systems which process automatically information relating to identifiable individuals should register. This requirement to register will apply to data users in both the public and the private sectors. The Lindop Committee found that registration schemes were a common feature of data protection legislation in other countries. A public register should go a long way to meet the objective that the existence and purpose of computerised personal information systems should be publicly known. The requirements for registration will be as simple as possible and it is expected that most applicants will be registered without question. The data user will normally be required to provide brief particulars identifying him, the information he uses, where it has come from and to whom it is disclosed, and the purposes for which it is used. He will also be required to register any changes in these particulars. The Registrar will have power to make enquiries, to inspect data files and to require modifications to a system. In extreme cases he may need to refuse registration on the ground that the applicants arrangements do not comply with the general principles. He will also be empowered if the case warrants it, to strike a data user off the register, and to take proceedings against data users (see paragraph 19 below).
10. The Registrar will be appointed by the Crown, and it is proposed that he should serve for five years in the first instance. He will be required to make an annual report to Parliament. He and his staff will be independent

of the Government, but the Government will designate him as the authority for rendering assistance to other Parties to the Council of Europe Convention.

11. Initially the Registrar may need a staff of about 20 (who should include computer experts) to set up the register as soon as possible after the legislation comes into force. While he will not have the resources to supervise the operation of data systems in detail, he will be expected to offer advice to data users and data subjects; to follow up cases where defects arise at the point of registration, to pursue complaints and give guidance on codes of practice.

Appeal Tribunal

12. The Registrar will have wide powers and it will be appropriate for there to be a right of appeal against his decisions. It is proposed that this should lie to an independent tribunal under a legally qualified chairman appointed by the Lord Chancellor. The members of the tribunal would be drawn from a panel which would include computer experts.

The Public Sector

13. Subject to the exemptions allowed in the legislation (see paragraph 17 below), central Government, local authorities, the police, nationalised industries and other public sector bodies will be required to register in the same way as other users. The register will clearly indicate the purposes for which these bodies use data relating to individuals and any arrangements for transferring such data from one organisation to another.

Special cases and exemptions

14. The power to make regulations (see para 8 above) will be needed to deal, amongst other things, with the processing of categories of data where it is not sufficient to rely on the general principles alone and where Parliament may expect to see detailed requirements laid down. Thus the Convention prohibits the processing of data revealing racial origin, political opinions or religious or other beliefs, health or sexual life

and criminal convictions unless the law provides appropriate safeguards. Some of these categories of data (and in particular medical records) may well need to be covered by regulations which might, for example, place special restrictions on the collection, processing, holding or disclosure of information from such records.

15. The collection and use of data solely for statistical or research purposes do not threaten the privacy of data subjects, provided that in processing and disseminating the results steps are taken against revealing information about an identifiable individual. For this reason, the principle that the data subject should have access to information held about him need not apply to records held solely for these purposes, nor need the information be absolutely accurate and up to date. This should apply equally to data specially collected for a statistical or research purpose and to data originally collected for administrative or other purposes.

16. The collection of information for the purposes of public records and other archives is already governed by specific legislation. It is not intended that the data protection legislation should inhibit the preservation of historically valuable data for these purposes.

17. The Convention permits derogation from the general principles (except in relation to measures to ensure the security of systems) in the interests of:

- "a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
- b. protecting the data subject or the rights and freedoms of others."

In accordance with the provisions at a. above it is proposed that the legislation should not apply to data that need to be safeguarded for the purposes of national security. The use of certain other data relating to the matters referred to at a. above will be exempt from registration.

These exemptions will include some data needed by the police for the prevention and detection of crime. Similarly, registered data users who make information available to the authorities in connection with these matters will not be required to register such disclosures of information. To register them would tend to defeat the purpose for which they are made. But the intention will be to keep exemptions from registration to the minimum that is consistent with the proper functioning of the law enforcement agencies. The provisions at b. above are likely to apply in the case of medical records and possibly in certain other areas such as sensitive information recorded by social workers. In such cases the user will have to be registered but it may be appropriate to restrict access by the data subject.

18. Those who use computer bureaux will have to register, as will the bureaux themselves. The latter will, however, be exempt from compliance with some of the general principles because it is not normally the bureau but the user who controls the purpose, collection, dissemination, and access to the data.

Sanctions

19. Criminal and civil sanctions will be tailored to fit the general principles of the scheme and to complement the powers given to the Registrar. It is proposed to make it an offence to make a false statement to the Registrar; to process personal information automatically without being registered or exempted from registration; or to fail to comply with a notice served by the Registrar regarding a defect to be remedied. For the most part the general principles are not expressed in language which would make it appropriate for their breach to constitute a criminal offence. But it is for consideration whether provision should be made for criminal sanctions where a data user deliberately records, uses or disseminates false information, refuses access to a data subject without good cause, or uses information for a purpose which is not registered.

20. The main purpose of the civil remedies will be to ensure that data subjects who have suffered damage because of a breach of the requirements governing data use can secure compensation, although injunctions will be

available to restrain breaches of a statutory requirement where damage is anticipated but has not yet been suffered. It is not envisaged that the Registrar will have any role to play in relation to civil proceedings, which will be the responsibility of the individual who alleges he has suffered damage. It is for consideration what form the liability should take. Liability dependent upon proof of fault would present difficulties for the plaintiff who would not often be in a position to adduce detailed technical evidence about the data user's operations. From the point of view of the plaintiff, some form of strict liability would be most effective. The form is again open for consideration: for instance, whether statutory defences might be available to the user, allowing him to avoid or limit liability where he had done all that was reasonable in the circumstances or could, perhaps, establish that he had not been at fault.

21. If complaints about public sector data systems relate to maladministration, whether or not they involve a breach of data protection, they may also fall to be investigated by the Parliamentary Commissioner for Administration or where appropriate the Parliamentary Commissioner for Northern Ireland or the Commissioner for Complaints in Northern Ireland. Where the relevant legislation applies complaints may also be taken up with the Health Services Commissioner or the Commissioner for Local Administration as the case may be.

Transfer of data to other countries

22. The legislation will include a power to restrict the transfer of categories of information to specified countries whose laws do not provide comparable safeguards for the privacy of computerised personal information in the categories concerned.

Costs

23. In accordance with the Government's objective of keeping the burden on resources to a minimum, everything possible will be done to ensure that neither the legislation or the regulations made under it impose unnecessarily costly requirements. In the public sector costs and manpower will have to be contained within existing planned totals, even if this means deferring

application of the legislation in some areas. The initial cost of the Registrar and his staff (see para 11 above) is likely to be of the order of £500,000 a year at 1981/82 prices. It is the intention that the fees charged by the Registrar will recover all his costs, including those of setting up the register. Every effort will be made to keep costs down, and the registration fees will represent only a minute proportion of the total cost of a data system.

24. Where a data subject is granted access to information relating to him he will normally be required to pay a fee designed to offset the costs of access. The access fee is a common feature of all European schemes. It should be large enough to deter frivolous or repeated requests for access, but not excessive in relation to the circumstances of data subjects.

25. An effective data protection system, however simple, is going to mean that some users incur increased capital costs for developing their hardware or software systems, and increased running costs as a result of responding to requests for access. But these implementation costs have to be balanced against the potential benefits. In particular data protection legislation is needed to ensure that the United Kingdom's substantial international trade in information, and its key role as a crossroads on the international data highway, are not compromised.

Timing of implementation

26. The registration process will take some time. It could be up to two years after legislation is in force before it is fully operative. A longer period may be necessary, for financial or other reasons (see para 23 above) before users of particular categories of data meet the full requirements of the legislation. The European Convention allows for phased implementation of data protection arrangements.

An Advisory Committee

27. Once the legislation is in force it might be appropriate to appoint an Advisory Committee to advise the Government on the preparation of

regulations relating to particular categories of data and, if the need arose, on possible changes to the legislation itself.

Conclusion

28. The Government believes that the proposals in this White Paper will safeguard privacy, protect our trading interests and enable the United Kingdom to ratify the Council of Europe Convention, and intends to legislate on these lines.

[Footnote: Any comments on these proposals should be addressed to the Home Office, E1 Division, Room 814, Queen Anne's Gate, London SW1.]

C A Whitmore Esq



CABINET OFFICE

With the compliments of
Sir Robert Armstrong KCB, CVO
Secretary of the Cabinet

✓ LM
27/1

70 Whitehall, London SW1A 2AS
Telephone: 01-233 8319

Ref. A07255

MR UNWIN

Thank you for sending me a copy of your minute of 25 January to Mr Rickett about data protection.

2. I wonder if I might refer you to paragraph 4 of my minute of 16 November 1981 (Ref. A06001), addressed to Deputy and Under-Secretaries. The relevant paragraph read as follows:

"As for requests from No 10 for advice on an ad hoc basis, I have agreed with the Prime Minister that these should in the first instance be directed to my office. I can then decide whether to submit the advice myself (on the basis of a draft commissioned from the Secretariat) or to ask one of you to do so direct."

3. I do not disagree with the advice which you gave in your minute of 25 January, but I should have preferred to have had a chance to see it, and if necessary comment on it, before it went to No 10. I should be grateful if, as a general rule, you could be guided by the relevant paragraph of my minute of 16 November 1981.

4. I am sending a copy of this minute to Mr Whitmore.

ROBERT ARMSTRONG

ROBERT ARMSTRONG

26 January 1982

CONFIDENTIAL

Home Affairs



Civil Service Department
Whitehall London SW1A 2AZ
Telephone 01-273 3000

Minister of State

The Rt Hon William Whitelaw CH MC MP
Secretary of State
Home Office
Queen Anne's Gate
LONDON SW1H 9AT

12 May 1981

Dear Willie,

*WM
13/5*

DATA PROTECTION

I have seen the letters of ~~17~~ March from John Nott and ~~2~~ April from Humphrey Atkins about the need to safeguard data collected for national security purposes.

There is a need also to preserve the confidentiality of those procedures that draw, for the purposes of national security, on data banks whose prime raison d'etre is not national security. This was considered by an official committee (the Personnel Security Committee) in 1979 in the context of the Lindop Report, and the points made then to your officials are, I believe, still valid.

I am copying this letter to the recipients of John Nott's and to John Nott himself.

Barney Hayhoe

BARNEY HAYHOE

CONFIDENTIAL

CONFIDENTIAL

Home Affairs



NORTHERN IRELAND OFFICE

GREAT GEORGE STREET,

LONDON SW1P 3AJ

SECRETARY OF STATE
FOR
NORTHERN IRELAND

2 April 1981

The Rt Hon William Whitelaw CH MC MP
Secretary of State
Home Office
Queen Anne's Gate
London SW1H 9AT

MP

Dear Willie,

DATA PROTECTION

In his letter to you of 17 March John Nott made the point that defence computers holding classified information should be exempt from any legislation on data protection.

Similar considerations on the grounds of security would of course be necessary in respect of some data held by the RUC in Northern Ireland, and I would endorse the importance of resolving this point before we ratify the European Convention.

I am copying this letter to the recipients of John Nott's letter and to John Nott himself.

Yours ever

Humphrey

CONFIDENTIAL

File

DS

Home Affairs

19 March 1981

As I told you on the telephone, the Prime Minister is content with the revised version of the statement on data protection enclosed with your letter of 18 March.

I am sending a copy of this letter to David Wright (Cabinet Office).

M. A. PATTISON

John Halliday, Esq.,
Home Office.



SCOTTISH OFFICE
WHITEHALL, LONDON SW1A 2AU

The Rt Hon William Whitelaw CH MC MP
Secretary of State for the Home Department
50 Queen Anne's Gate
London
SW1H 9AT

✓
18 March 1981

Dear Willie,

GOVERNMENT STATEMENT ON DATA PROTECTION

I refer to your letter of 11 March to Patrick Jenkin to which was attached the draft of a statement by the Government that we have decided, in principle, to introduce legislation on data protection as soon as an opportunity offers.

On a minor point of detail, I feel that the draft question could be improved by the insertion of "personal" before "information". This would provide a more accurate description of what is intended. I am content with the statement as it stands, and I note especially that it includes no reference to National Health Service records. The extent to which the proposed legislation should be applied to the National Health Service must however be subject to careful consideration in due course. In particular, I shall want to be satisfied that there will be effective safeguards governing access by patients to information about them on medical records.

I am copying this letter to Patrick Jenkin and the other recipients of your letter of 11 March.

Yours ever,

George



HOME OFFICE
QUEEN ANNE'S GATE LONDON SW1H 9AT

18 March 1981

MS
Prime Minister

Dear Mike,

DATA PROTECTION

The data protection statement will be given tomorrow. You may like to be aware of 'x'!

The Home Secretary has considered the comments made on the draft statement circulated with his letter of 11 March to the Secretary of State for Social Services. I now enclose a copy of the statement, which has been revised to take account as far as possible of those comments.

MP 18/3

x | The question of importance, which the Secretary of State for Industry and Mr. Ibbs raised, was whether the statement should declare at this stage the Government's intention not to set up an independent data protection authority. The Home Secretary took the view that questions were bound to be asked about the Government's intentions in this respect, which would have to be answered, and that it would be better to declare the position now than to appear to admit it reluctantly later. I understand that Sir Keith Joseph and the CPRS have accepted that the statement should make the position clear.

An arranged Question is being tabled today and will be answered tomorrow at 3.30 p.m.

Copies of this letter and its enclosure go to the Private Secretaries to the members of H Committee, the Foreign and Commonwealth Secretary, the Secretary of State for Industry, the Secretary of State for Defence, Sir Robert Armstrong and Mr. Ibbs.

Yours ever,
John Halliday
J. F. HALLIDAY

M. A. Pattison, Esq.

To ask the Secretary of State for the Home Department whether the Government proposes to introduce legislation to safeguard personal information handled automatically and to make a statement.

DRAFT REPLY

The Government has decided in principle to introduce legislation for this purpose when an opportunity offers.

The Government is satisfied that developments in information technology make it desirable to provide statutory protection for personal information handled automatically. In reaching this conclusion the Government has had regard to developments internationally and in particular to the guidelines on this subject adopted last autumn by the Organisation for Economic Co-operation and Development and to the Convention concluded by the Council of Europe. The legislation will enable the UK to endorse the OECD guidelines and to ratify this Convention. In the meantime, the Government proposes to sign the Convention at an early date.

The Government accepts as a starting point the principles formulated by the Younger Committee in its report on Privacy (Cmnd 5012 paras 592-599). Our intention is that the legislation should incorporate and so far as possible give effect to these principles. Consultations following the publication of the report of the Data Protection Committee under the chairmanship

of Sir Norman Lindop (Cmnd 7341) showed broad acceptance of the need for some statutory control but less agreement about the machinery. One of the Government's objectives will be that our arrangements should keep additional demands on resources to a minimum. We do not therefore propose to set up an independent data protection authority. Another objective will be that the arrangements should be sufficiently flexible to allow for differences between automatic processing methods, the purposes of data systems and the information they contain.

The basis of our proposals will be the establishment of a public register. This will be built up in stages. Users of systems which handle personal information automatically will be required to register and to comply with various other requirements.

The intention is that registration should require, as a minimum, a description of the system and the purposes for which it is used and publication of the code of practice followed by the user. Provision will be made to ensure that adequate security arrangements are observed. There will also be provision for securing access to information by data subjects as appropriate. There will be full consultation with trade associations and other bodies about the progressive implementation of the requirement to register. The legislation will also provide for appropriate sanctions to ensure compliance with these requirements.

RESTRICTED



✓ MJD

MINISTRY OF DEFENCE WHITEHALL LONDON SW1A 2HB

TELEPHONE 01-218 9000
DIRECT DIALING 01-218 2111/3

MO 26/2/1

17th March 1981

Dear Willie

DATA PROTECTION

Thank you for copying to me your letter of 11th March to Patrick Jenkin.

I have only one Departmental point to make. You will readily understand that there are significant defence interests involved here, and we will need to seek appropriate safeguards to ensure that our interests are adequately protected. In particular, I think defence computers holding classified information should be exempt from the proposed legislation. This point will need to be pursued further by officials, and it is important that it is resolved by the stage when we would ratify the Convention.

I am sending copies of this letter to the Prime Minister, to other members of H, to the Foreign and Commonwealth Secretary, the Secretary of State for Industry, the Secretary of State for Trade; and to Sir Robert Armstrong and Mr Ibbs.

John Nott

John Nott

The Rt Hon William Whitelaw CH MC MP

RESTRICTED



✓
MAD

CABINET OFFICE
Central Policy Review Staff

With the compliments of
J. R. Ibbs

70 Whitehall, London SW1A 2AS
Telephone 01-233 7765



Home Affairs

CABINET OFFICE
Central Policy Review Staff

70 Whitehall, London SW1A 2AS Telephone 01-233 7765

From: J. R. Ibbs

Qa 05287

16 March 1981

Dear Secretary of State,
Data Protection

Thank you for sending me a copy of your letter of 11 March to the Secretary of State for Social Services enclosing a draft statement on data protection.

I have one significant concern and several minor suggestions.

My concern relates to the sentence at the end of page 1, where it might be better to omit the words "and it does not therefore propose to set up an independent data protection authority". First, it is a sound principle to avoid saying what the Government will not do until it is in a position to say what it will do. Second, we may yet find that the other members of the Council of Europe will press us to establish an independent authority to provide equivalent protection to theirs, if we are not to be at a severe disadvantage through being denied international data flows.

I attach for your consideration a possible re-draft which uses the language of information technology somewhat more precisely and tries to avoid giving unnecessary hostages to the civil liberties lobbies.

I am sending a copy of this letter to the recipients of yours.

Yours sincerely,

J R Ibbs

The Rt Hon William Whitelaw CH MC MP
HOME OFFICE
S W 1

DRAFT WRITTEN QUESTION AND ANSWER

To ask the Secretary of State for the Home Department whether the Government proposes to introduce legislation to safeguard personal information which is handled automatically and to make a statement.

DRAFT REPLY

The Government has decided to introduce legislation for this purpose as soon as an opportunity offers.

The Government is satisfied that developments in information technology make it desirable to provide statutory protection for personal information which is handled automatically. In reaching this conclusion the Government has had regard to developments internationally and, in particular, to the guidelines on this subject adopted last autumn by the Organisation for Economic Co-operation and Development and to the Convention concluded by the Council of Europe. The legislation to be introduced will be intended to enable the UK to endorse the OECD guidelines and to ratify this Convention. In the meantime, the Government proposes to sign the Convention at an early date.

The Government accepts as a starting point the principles formulated by the Younger Committee in its report on Privacy (Cmd 5012 paras 592-599). Its intention is that the legislation should incorporate and give effect as far as possible to these principles. Consultations following the publication of the report of the Data Protection Committee, under the Chairmanship of Sir Norman Lindop (Cmd 7341) showed broad acceptance of the need for some statutory control but less agreement about the machinery of control. One of the Government's objectives will be that the arrangements should keep additional demands on both Government's and businesses resources to a minimum. Another objective will be that the arrangements should be sufficiently flexible to allow for differences between automatic processing methods, the purposes of systems and the information they contain.

The basis of the Government's proposals will be the establishment of a public register which will be built up in stages. Owners and operators of systems which handle personal information automatically will be required to register their systems and to comply with various other requirements.

The intention is that registration should require, as a minimum, a description of the system and of the purposes for which it was, or was intended to be, used and

a declaration that it would be operated according to a published code of practice. Provision will be made to ensure that adequate security measures were taken to protect data from unauthorised access. There will also be provision for data subjects to gain access to information about themselves if appropriate. There will be further consultation with trade associations and other relevant bodies about the progressive implementation of the requirement to register. Legislation will provide for appropriate sanctions to ensure compliance with these requirements.



file No

10 DOWNING STREET

From the Private Secretary

16 March 1981

The Prime Minister has seen a copy of the Home Secretary's letter of 11 March to the Secretary of State for Social Services, about the proposed Government statement on the principle of legislation to set up a scheme for data protection.

She is content, subject to drafting points which may be raised by colleagues.

I am copying this letter to David Wright (Cabinet Office).

M. A. PATTISON

A. P. Jackson, Esq.,
home Office.

9



DEPARTMENT OF HEALTH & SOCIAL SECURITY

Alexander Fleming House, Elephant & Castle, London SE1 6BY

Telephone 01-407 5522

From the Secretary of State for Social Services

ms

The Rt Hon William Whitelaw CH MC MP
Secretary of State for the Home Department
53 Queen Anne's Gate
LONDON SW1

16 March 1981

ms

Prime Minister

*Mr Jenkin's programmes
will be one of the difficult
areas for data protection
legislation. MJP/18/3*

Dear Willie,

DATA PROTECTION

Thank you for your letter of 11 March.

I note your intention to announce that the Government intends to sign the European Convention at an early date and your view that we could not avoid applying such legislation to the National Health Service in due course. I read the proposed statement and your letter as meaning that the legislation would leave open the form and timing of this. This is very important in relation to the sensitive area of personal medical information, where we should want to have full discussions with the medical profession - who have been taking a very active interest in data protection - and to carry them with us on the form of the arrangements. We may also need to consult other professional interests. All this may have implications for the actual content of the legislation and no doubt we shall be consulted on your detailed proposals. (I have also seen the suggested re-draft by CPRS attached to Mr Ibbs' letter of 16 March to which the above considerations would be equally applicable.)

I must again draw attention to the possible resource consequences to all the programmes for which I am responsible and reserve the right to seek additional resources to cover these. In one particular, I must make clear that we cannot give people access to information contained in their social security records and at the same time be sure of meeting the Government's manpower target to reduce the Civil Service to 630,000. Social Security records cover virtually the whole population and there are therefore potentially huge manpower implications for my Department from requests for the information they contain.

The proposed statement is bound to arouse the interests of the British Medical Association and when it is made I shall need to write to them to assure them of our intention to consult the profession. I shall be grateful therefore if your officials could keep in touch with mine about the timing of the statement.

*Your ever
Peter*



✓ Press

Told H.O. by
'name that
PM has no objection.

QUEEN ANNE'S GATE LONDON SW1H 9AT

1.

Dear Patrick

Ann
no

11 March 1981
Prime Minister
we have seen no comment
from others. Content for Home
Secretary to issue written answer?

MAJ
13/3

As you know, the Home and Social Affairs Committee decided on 10th February that it agreed in principle to legislation to set up a scheme for data protection on the lines of my proposals. It invited the Home Office to circulate to the Committee the draft of a Government statement on the subject.

My officials have consulted officials in your Department and in other Departments concerned. The enclosed draft statement takes account of their comments, although it has not been possible to adopt all of them. You will see that the statement does not refer to the National Health Service. I ought to say, however, that having decided to announce our acceptance in principle that legislation on data protection is desirable I do not see how we could ratify the Convention without being prepared in due course to apply the relevant legislation to the National Health Service.

As you will see, I propose to announce that the Government intends to sign the European Convention at an early date. The implication of this is that we ought to proceed to signature as soon as possible after the announcement has been made. Having decided to bring forward legislation with a view to ratifying the Convention there seems no point in continuing to keep options open and considerable advantage in making clear the genuineness of our intentions by signing the Convention. Unless you or any of the other recipients of this letter indicate to the contrary, therefore, we will assume that your concurrence in the statement announcing an intention to sign the Convention shortly extends to going ahead with the signature itself in the next month or so.

There would be advantage in an early announcement. I should therefore like to be able to take it that you, and others to whom I have copied this letter and enclosure, are content if I do not hear from them by close of play on Monday 16th March.

I have sent copies of this letter and enclosure to the Prime Minister, to other members of H, to the Foreign and Commonwealth Secretary, Secretary of State for Industry, Secretary of State for Defence, Secretary of State for Trade, and to Sir Robert Armstrong and Mr. Ibbs.

John M.
Lester

The Rt. Hon. Patrick Jenkin, M.P.

E.R. • DRAFT WRITTEN QUESTION AND ANSWER

To ask the Secretary of State for the Home Department whether the Government proposes to introduce legislation to safeguard information in computerised data systems and to make a statement.

DRAFT REPLY

The Government has decided, in principle, to introduce legislation for this purpose as soon as an opportunity offers.

The Government is satisfied that developments in information technology make it desirable to provide statutory protection for personal information which is handled automatically. In reaching this conclusion the Government has had regard to developments internationally and, in particular, to the guidelines on this subject adopted last autumn by the Organisation for Economic Co-operation and Development and to the Convention concluded by the Council of Europe. The legislation to be introduced will be intended to enable the UK to endorse the OECD guidelines and to ratify this Convention. In the meantime, the Government proposes to sign the Convention at an early date.

The Government accepts as a starting point the principles formulated by the Younger Committee in its report on Privacy (Cmnd 5012 paras 592-599). Its intention is that the legislation should incorporate and give effect as far as possible to these principles. Consultations following the publication of the report of the Data Protection Committee, under the Chairmanship of Sir Norman Lindop (Cmnd 7341) showed broad acceptance of the need for some statutory control but less agreement about the machinery of control. One of the Government's objectives will be that the arrangements should keep additional demands on resources to a minimum and it does not

E.R. .

therefore propose to set up an independent data protection authority. Another objective will be that the arrangements should be sufficiently flexible to allow for differences between automatic processing methods, the purposes of systems and the information they contain.

The basis of the Government's proposals will be the establishment of a public register which will be built up in stages. Users of computerised personal data will be required to register and to comply with various other requirements.

The intention is that registration should require, as a minimum, a description of the system and of the purposes for which it was used and the publication of the code of practice followed by the user. Provision will be made to ensure that adequate security arrangements are observed by registered users. There will also be provision for securing access to information by data subjects as appropriate. There will be full consultation with trade associations and other interested bodies about the progressive implementation of the requirement to register. The legislation will provide for appropriate sanctions to ensure compliance with these requirements.

Home Affairs

PRIME MINISTER

You were interested in all three items at this H
meeting.

The committee decided to go for data protection
legislation. Details and timing are far from settled, but
the importance of the decision is that the principle has
now been agreed and can be announced. This will help to
protect us against loss of industries to countries which
are already taking steps in this direction.

The committee agreed to resist the application to the
European Human Rights Commission over the Leasehold Reform
Act 1967.

The Home Secretary has already reported to you on the
discussion of management of public sector higher education.
The minutes record in more detail the concerns of those who
oppose Mr. Carlisle's scheme. I am told that the minutes have
been drafted to convey a greater sense of balance in the
discussion than was actually present.

12 February 1981

PRIME MINISTER

1. DL to see Home Affairs
2. CS to see re meeting
CS 8/12 MP 8/12

See Ind Pd
Jan 80
Information -
Technology
A need
mt

E Committee is to discuss information technology in about 10 days time. I know that Robin Ibbs and ^{DR} John Ashworth will be asking for an opportunity to talk to you for 10 minutes in advance of the meeting, because they are concerned that there is no effective central grip on this field in Government yet.

Another information technology problem is currently being handled in H Committee. This is the matter of possible legislation on data protection. The forum is an unfortunate one because few of those who attend really understand the implications. I think it would be useful for you to be aware of the issues raised. I attach a note from John Hoskyns describing his researches about the state of the discussion, together with the minutes of the H discussion.

MP

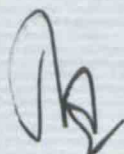
5 December, 1980.

MR PATTISON

H MEETING ON DATA PROTECTION

You asked for comments on the minutes of H Meeting on 2 December.

1. From the minutes, it seemed to be a peculiar discussion, blowing warm with Raison, backed up by Downey, blowing cold in discussion and then luke warm again in conclusions (that Trade and Industry should consider further with CPRS).
2. I talked to Gordon Downey who said that it was indeed a peculiar meeting and that the Home Secretary was obviously dissatisfied that Trade and Industry had not been properly represented at the meeting. H is full of non-Industry people who were not properly briefed, did not really understand the issues.
3. Data protection is very important. There almost certainly will be international penalties if our data protection code/legislation is not in line with that of other countries (apparently the Americans are already running into trouble), but it is really a Government-to-Government incompatibility that we have to worry about. The fact that, as yet, individuals don't really fuss too much about it is not the point. Of course some systems (eg the police system at Hendon with which my own old company was heavily involved) are highly sensitive, but there should be no difficulty in excluding certain systems from codes/legislation where national interest applies.
4. The Home Office are always very conservative about this sort of thing, and no doubt worry that they might be losing control in such sensitive areas. But the trade penalties could be real.
5. Conclusion i. in the minutes shows that the door is open. Trade and Industry will be doing further work with CPRS and expect to produce a paper demonstrating with chapter and verse that some legislation will be necessary.



JOHN HOSKYNS



IT8.7/2-1993

2009:02



IT-8 Target

Printed on Kodak Professional Paper

Charge: R090212