DATA PROTECTION

The monster that just grows

In a discreet Mayfair building, MI5 is busy setting up a gigantic secret State databank — with the facility to tap into our personal files in other government departments. DUNCAN CAMPBELL reports on his investigation with STEVE CONNOR of 'Computing' magazine.

MI5, THE Security Service, have over the last four years put into operation the largest government databank in Britain. Their Mayfair-based computer has a storage capacity sufficient to hold files on 20 million people, and is linked to a growing network of other government computer databanks. MI5's taps into other government files are licensed by a Charter from the Prime Minister. This Charter and other links, both secret and announced, between government-held personal files have enabled officials to start building what could ultimately be a comprehensive national filing system on each individual. The main links between government files so far have been based on the use of names and National Insurance numbers. Four key departments holding personal information – the Inland Revenue, the Department of Health and Social Security, the Department of Employment, and MI5 – have passed information between themselves in this way.

Home Office Minister Timothy Raison has promised that the government will publish a White Paper on data protection and privacy this spring. The White Paper is a response to the report of the Data Protection (Lindop) Committee in December 1978, which recommended the creation by parliament of a powerful and independent authority to regulate the storage and use of personal information on computer. The recommendations include complete control over police databanks, even those concerned with criminal intelligence. The committee even suggested that MI5's computers should be supervised by a security-cleared privacy consultant appointed from the new Data Protection Authority.

The Home Office intends to accept none of this, and to exempt all police and security service systems from outside scrutiny. Our investigation has revealed some of the reasons for the government's determination to keep the wraps on MI5:

● The data storage capacity of the computers, estimated to cost between £15 and £20 million, is two and a half times that of the already controversial Police National Computer. The PNC itself has forty million personal records, and is checked tens of thousands of times daily. Information has often leaked from it.

● MI5's access to other departments' files is unlimited, according to details in their Charter which have been published in Australia, but never before in Britain. The Charter also says that their information system should be 'comprehensive'. The Ministry of Defence has stressed, in unpublished evidence to the Lindop committee, that new data protection laws should allow exemption so that the security services have access to personal data files held elsewhere in government.

● MI5's files are in addition to more than 1.3 million Special Branch files already on computer at New Scotland Yard. This system, which was known to the Lindop committee, provoked for them 'new dimensions of unease'.

● Development work on MI5 computers and associated networks to tap into other government computers has been under way since before 1972. A succession of plans to create a network of central government computers has been tested – and, a computer executive from ICL says privately, is under active development within the company. The person in charge of the project, Mr Trevor Davies of ICL, told us last week: 'I'm sworn to secrecy'. Unofficial sources say that the network gives or will give MI5's computers direct access to the records of the DHSS, Inland Revenue and other departments.

THE CENTRE of MI5's computing operation is a discreet, modern building on a quiet Mayfair side street called Mount Row. Although the building bears no notice of ownership, surly doorkeepers claim that it is the 'Ministry of Defence'.

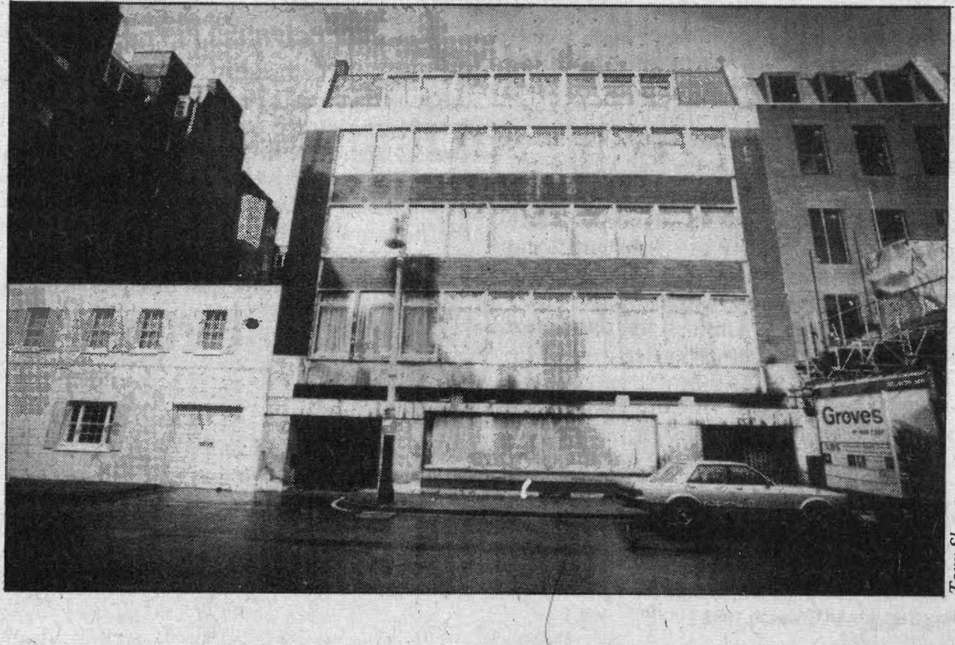
But 26-28 Mount Row, W1 is not used by any orthodox department of the MoD. The government's extensive central London property portfolio records its usage as 'MoD-X Computer Centre'. The 'MoD-X' allocation, meaning Department X of the MoD, is in fact an artless and useless attempt to conceal the building's actual use by the Security Service.

Inside, behind immense metal doors and layers of security guards, is the centre of the complex. It appears to have come into operation in the early 1970s, equipped with the then largest British-made computer, an ICL1907. Just over four years ago, as ICL negotiated to supply a new machine, an over-enthusiastic ICL employee leaked news of the impending new order to a trade magazine, *Computer Weekly*. Neither ICL nor the MoD would then comment further, except to say that the task was to maintain a 'classified database'. The story died.

The computers ordered by the 'Ministry of Defence' were a double or 'dual' ICL 2980, largest of the companies' powerful 'new range', plus a 2960 (for 'back up'). The most formidable part of the MI5 specification was for a huge 'disc store'. There were to be over 100 disc store units of ICL's type EDS200 – the largest then made. This electronic memory, even by the standards of an industry accustomed to superlatives, could only be called gigantic. Together, these discs can store 20 thousand million characters, letters or numbers; 20 'gigabytes' of information. This is equivalent to the information in a library of about 50,000 paperback books. Or, it could store personal dossiers on some 20 million people, if these consisted of identifying particulars and about 150 descriptive words.

Neither the Ministry of Defence nor ICL deny that this order was fulfilled. ICL's chief press officer told us that three such dual ICL2980s had been delivered, worldwide. Two had gone abroad and one had been for 'a government department,

In government records, the MI5 building at 26-28 Mount Row, Mayfair, is listed as 'MoD-X Computer Centre'. Staff reach the computer equipment by passing through massive ground floor steel doors, which are always kept locked.



Tony Sleep

somewhere in the United Kingdom'. An MoD spokesman said last week that the computer did indeed exist as specified and is 'in use in the intelligence field. We can't say any more'.

We have confirmed that ICL engineers work both at Mount Row and at the MI5 HQ in Curzon Street, a short distance away. Engineering staff at Mount Row include a Mr Jeff Chandler who is attached to ICL's control centre in Clifton Street, London – although his name is not, apparently, listed in the company's central personnel records.

THE NETWORK of government computers has been under development over the last ten years. MI5's earlier computer was known obliquely within ICL as MoD-Mult, suggesting that the plan always contained the proposal for a multiple computer network. An official with the government's Central Computing Agency (now the Central Computing and Telecommunications Agency) told us that during the first half of the 1970s there were two highly classified, virtually 'nameless' projects within the agency. The first was a Royal Navy computer which controls their ships, including Polaris submarines. The second was 'the place in Mount Row' which was MI5.

Experiments in computer linkage begun in the early '70s have become, in some aspects, quite public. By 1973, the Central Computing Agency and ICL were developing a prototype 'General Administrative Network' – or 'GANNET' – to link up computer centres across Britain. Another project for the Ministry of Defence, GRID 77, anticipated a national network based on four centres starting operation by 1977. But several ICL sources directly linked these projects, whose outline was publicly known, with highly classified work on links for MI5. One executive named Mr Trevor Davies of ICL as the manager.

Mr Davies, who works at ICL's offices in Derry Street, London, said last week that he was 'sworn to secrecy'. It was, he agreed, a government computer network, but 'not for the Ministry of Defence'. Which government department then? 'I'm sorry, I can't tell you anything'.

A 1975 White Paper on 'Computers: Safeguards for Privacy' reported that a government interdepartmental working party had examined 'all information held, or likely to be held, in computer systems of Government Departments, and the rules governing its storage and use'. It was then claimed that the idea of linking computers together had been discarded.

Shortly after the White Paper was published, however, a report by the US Congressional Subcommittee on Government Operations, on 'Privacy and Protection of Personal Information in Europe', observed, after making official enquiries, that this wasn't quite the case:

> Under the direction of the Central Computer Agency (and) the Home Office, the technical feasibility for linking several data systems (and record comparability and standardisation) is being studied.

Soon after the White Paper was issued, ICL staff were being offered jobs on MI5's 'upgrade' programme to plan the installation of the huge, new computers.

At the same time, the government was deeply involved in studying the problems of linking large computers into networks, to exchange information and instructions. The network plans were developed simultaneously in both civil and military departments. The Ministry of Defence had, by 1972, a GRID 77 Feasibility Study (GRIDFEST) under way in East Anglia.

The GANNET project began in 1973. It was based at the government's Central Computer Bureau in Norwich, and was linked to DES computers at Darlington, among others. When the first GANNET closed down around 1976, two things happened: a new, (and innocuous) network using the system was set up between Northwestern Universities' computer centres; and, according to a GANNET specialist, the Ministry of Defence 'took the code' in order to run its own GANNET.

The GRID 77 project was not a success, and only one of its network centres, called Bureau West, was ever built. Located at Devizes, Wiltshire, Bureau West also houses two 2980 ICL computers, and originally operated the Royal Navy's main stores and supplies system. But the effect of these developments has been to provide a system, on which ICL is clearly continuing to work, which can set up links between different government computer centres.

MI5 HAVE AUTHORITY from the Prime Minister for its taps into other government databanks. Not even the 1975 White Paper denies this, merely noting that the 'exceptions' to their assurances and comments 'are computer systems kept for the strict purposes of national security: these are not described here'. MI5's computer was, of course, not listed.

The Security Service's authority to snoop freely in government records comes from a still-secret part of its Charter, which gives the Director-General the power to see any records:

> 10. You will arrange to have such access to the records of Government Departments and agencies as you may deem necessary for the purposes of your work.

These words have never before been published in Britain. They were recently unearthed, in a remarkable piece of detective work, by Tony Bunyan of the State Research Group, who examined provisions made in Australia for setting up their own security services, at British request, in 1949. Their Charter, eventually published in a 1977 report, was a copy of MI5's.

Other parts of MI5's charter have been published, after they were incorporated into a 1953 Directive to the then new Director-General, and published 10 years later in Lord Denning's report of the Profumo scandal. However the critical passages referring to MI5's files were omitted: The rest of the section gave a Prime Ministerial directive to MI5 to set up their security filing system as widely as possible:

> You will establish a comprehensive set of security records. In order to do this you will arrange that all Government Departments and agencies submit to you for inclusion in your records all information bearing on security which may be, or come into their possession.

This licence for untrammelled information gathering has continued into the computer age. MI5's continuing access to government files was indirectly referred to in 1977 when the Data Protection Committee received evidence from the MoD. Although the full evidence was not then published, copies of it have now been made available. These show that when the MoD was asked about a potential law requiring the purposes of information storage on computer to be confined to those for which the subject had given the data in the first place, they said that it was 'essential that exemption should cover all computerised information concerned with security matters.'

THE DEVELOPMENT of the 'MoD-X' centre has been costly. The computers alone cost around £5 million – without accessories – according to ICL. Overall, the costs of the centre so far must have been at least £15 to £20 million. The money to pay for such equipment is carefully disguised within the Ministry of Defence budget, under longstanding arrangements for such laundering of funds. (The well-known 'Secret Vote' is separate from this and is used only for activities which must be unaccountable even within government, such as bribes and payments to informants.) Questioned by a House of Commons committee two years ago about such 'laundered' payments in his budget, MoD Permanent Secretary Sir Frank Cooper claimed that such arrangements were legitimate and had had the permission in 1946, if no more recently, of the Public Accounts Committee. The covert use of MoD funds for such activities as MI5's were, in his view, 'fully accountable in every sense of the word'.

The claim is a strange one, since no questions about MI5 are ever even accepted to be asked in parliament. The case of the MI5 computer centre is particularly apposite since at the time it was ordered ICL2980 computers already supplied to the MOD had been heavily criticised for their lack of reliability and performance.

THE CRITICAL QUESTION about the 'MoD-X Computer Centre' is of course the use to which they put the computer. What exactly does it store, about whom, and for what purpose is the information kept and used? A challenging point is the sheer difficulty of accumulating the vast amount of information to be stored. You would, one specialist pointed out, need 'an army of monkeys' at work for several years to amass so much. A likely explanation is that the computer store includes records and other material built up by the first MI5 computer; and that it has copied large amounts of information from other computer systems, or received it from automatic electronic systems, particularly surveillance systems.

Specialists with knowledge of security and intelligence agencies concur that the most likely application would have been to put all MI5's files on computer – personal dossiers, agent and outside reports, even public source cullings such as clippings from left-wing papers – and to apply to all of these a powerful computer method to examine and later, possibly, predict what is happening. A major part of this is a technique called Free Text Retrieval which enables data on any subject or combination of subjects to be retrieved rapidly from a huge database.

The use of FTR would partially explain the size of MI5's computer files. Such systems often use many times the basic storage requirement in order to operate. They also introduce, according to the Lindop Committee, 'new dimensions of unease'. FTR systems, the Committee's 1978 report observed,

> provide an easy method of browsing through collections of information (and) are well suited to surveillance requirements such as criminal intelligence or the preservation of national security . . . They are ideally suited to the retrieval of every occurrence of particular items of information from a large mass, and for discovering the relationship of one piece of information with another.

FTR systems greatly concerned the Data Protection Committee, and when they were used on personal information databases they presented 'special problems of definition and control.' But they are ideal for any agency concerned in maintaining as wide – and as automated – a surveillance system as possible. Anything at all could be thrown into the 'unstructured' files used by FTR. And 'unstructured files place virtually no constraints on the quantities or type of data which may be stored.'

THE POTENTIAL CATCH from trawling for information in government databanks is immense. By 1980, there were over 200 separate computers in use for 'general and administrative purposes' by central government. The 1975 White Paper listed 220 databanks with information about people outside government employment.

The DHSS, Inland Revenue, Department of Employment and the police routinely amass huge quantities of personal information. The Inland Revenue's 'Centre 1' at East Kilbride, near Glasgow, maintains millions of PAYE records. But it is still not 'on-line' so that information can be retrieved instantly – not even for IR staff – and so an MI5 linkup must still be on the drawing board.

The Inland Revenue refused this week 'to confirm or deny' whether information was openly available to the Security Services. There was a 'general rule' of privacy with 'statutory exceptions'. But did MI5 have access? 'I am not denying it. There is a general rule and there are statutory exceptions. You will have to be satisfied with that.' Most Inland Revenue files are still maintained manually on 'Con (for control) Cards' which give basic tax details and personal circumstances of each person. 'Ironically', according to one source, 'it's easier and faster to get the information by phoning the clerk with the Con Cards' than it would be if the records had been computerised.

The Inland Revenue admit that much of their data on an individual is automatically transferred to the DHSS (and sometimes by computer cards) because of the unified system for collecting PAYE tax and graduated NI contributions. The principal DHSS computers are located in Newcastle, and linked directly to local offices and other DHSS computer centres. Although the nation's 40 million NI records are kept in Newcastle, benefit payments are sent from other DHSS computers in Reading and Livingston, Scotland.

The DHSS are the logical focus for central government databanks. Two developments have created a high degree of centralisation already: the DHSS receives detailed information about income from the Inland Revenue because of graduated contributions arrangements; and the linking of unemployment benefit and social security payment systems has created similar links with the Department of Employment. A 1980 report by the DHSS, called 'A Strategy for Social Security Operations', recommended a central databank, styled the 'Whole Person Concept'. It had administrative advantages:

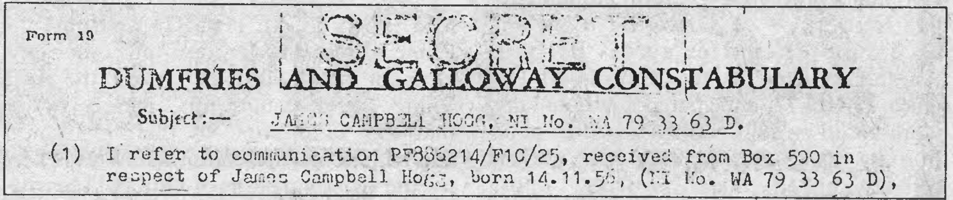
> 1.1 All relevant data about the person concerned held by the Department should be readily accessible at the point of enquiry or claim.
> 1.2 The records of spouses (and other people with adult dependants) should be suitably cross-linked . . .
> 1.3 Child Benefit records should be cross-indexed to the records for both spouses .

Last year, a Rayner report to the Prime Minister recommended complete integration, on computers, of Inland Revenue and DHSS information. The report suggested this could follow the complete computerisation of PAYE in the mid-1980s.

The DHSS is not unaware of the social tensions that such moves may ultimately create. Its new computer centre in Reading, due to be completed this year, has no windows on the ground floor. When police hunting the Yorkshire Ripper were given access to over 17,000 computer records at the Newcastle centre three years ago, DHSS officials publicly stressed that this should be a 'one-off exercise'.

The DHSS said this week that MI5 can have access to its personal information files, 'in cases of national security', but claimed that it was not possible for them 'just to plug in'. The matter of what could be transferred was 'one of these awkward questions'.

THE KEY to the linkage of personal files on different government computers is the National Insurance number – a code usually allocated the first time you are employed or claim benefit. Every adult has to have one. And although they were intended for a completely different purpose, MI5 have adopted them as a convenient index of adult Britons. This was clearly shown when, two years ago, a London magazine was inadvertently sent a copy of a letter from Special Branch detectives in Dumfries to Box 500 in London – a standard codename for MI5. MI5 had sought information about a young left-wing shop steward in the Dumfries area, James Hogg. To each reference to his name was appended his NI number. The NI number has become MI5's reference scheme for its files, and an ideal way to obtain basic data for its 'comprehensive' records. Anyone claiming benefits or in employment will be on the Newcastle computer, through which full basic personal information is available to MI5.



Form 19

SECRET

DUMFRIES AND GALLOWAY CONSTABULARY

Subject:— JAMES CAMPBELL HOGG, NI No. WA 79 33 63 D.

(1) I refer to communication PF886214/F1C/25, received from Box 500 in respect of James Campbell Hogg, born 14.11.56, (NI No. WA 79 33 63 D),

James Campbell Hogg, 24, had committed no crime – but was investigated by Special Branch in Dumfries on orders from 'Box 500' – one of MI5's aliases. His National Insurance no. was used as a personal identifying code.

The *New Statesman* has obtained documents showing that secret data linkage, using NI numbers, has taken place for some years. The DHSS has prepared statistical tables since at least 1980 which, according to a government memorandum, are 'derived from the linkage of Inland Revenue PAYE data and DHSS National Insurance Information'. It warned that:

> These data are supplied to us on the strict understanding that they are for use within this department only and that no reference to them, not even to the existence of them, will be made to persons outside the Department

The way ahead – if computer databanks continue to proliferate unsupervised – is clear. So are the government's intentions. By the time anyone has woken up to the effects of the MI5 dossiers and the linked personal files, it will be too difficult and too costly to change things. More than ten years have passed since the first Royal Commission, under Sir Kenneth Younger, recommended legislation to protect privacy. Now, a mouse of a White Paper is offered to forestall any action on the subject. The White Paper, as presently drafted, will evade the critical issues which ultimately affect society rather more deeply – the keeping of files about political beliefs and activities (which, bluntly, is a large part of what MI5 is about) – and the linking of computer dossiers. These issues should now come to centre stage. □