NEW
24 April 1987 IR£1.34 US$1.50 By Air 90p
STATESMAN

- Is disarmament possible? • Hitchens on Reagan
- Sugar women of Bombay • Radio renaissance
- The strain in Spain • Comics • Pop

BLACKS & THE LEFT: New relationship needed

SECRET SOCIETY

DUNCAN CAMPBELL's Report on Britain behind closed doors. Part One: Personal data for sale.

Cover illustration: Simon Stern

1. The databank dossier

As Britain stands, irreversibly, on the brink of establishing a chain of private and public national computer databanks,* DUNCAN CAMPBELL *proves that people* do *care about their privacy

WHAT IF? . . . What if someone put together everything known about you in each official file and from every government computer, and assembled it into one big data dossier? What horrors would be there?

Such an exercise is fictional, and its results are false. Worse, by concentrating on exotic and speculative data, it traduces entirely the very serious concern that people have about how simple and basic information about them is held and used by others without their permission. It's not just central government that has established large and worrying databanks. Over the last five years, two commercial companies have set up larger databanks than those currently operated by the police, Inland Revenue, or DHSS. These commercial databanks have information on every adult in the country, almost without exception. With 43 million people on file in their giant computers, and 17,500 access terminals, there is already a commercial market for personal information annually worth tens of million of pounds.

Very soon, these private population registers will be followed by larger government systems. Joint registers between the Inland Revenue and the DHSS are already well established. New health computer databanks will in due course form another, integrated national network. Future government proposals to replace local rates with a compulsory individual poll tax or 'community charge' depend on setting up a computerised register of everyone who uses local authority services. An integrated 'Government Data Network' is to be introduced, according to a government announcement in January. So gradually, the newspaper fiction of a single 'Big Brother' computer system will become substantive fact.

The significance of the giant computers is enhanced by technological leaps in the speed of computing, and the reducing expense of information storage. *This progress is not matched by equivalent improvements in security and data protection. During the* Secret Society *investigation, we exposed a ring of people tapping information from police and government databanks.*

But the government wasn't prepared to co-operate at all with any of our enquiries. When *Secret Society* asked the Inland Revenue, DHSS and Home Office to show and talk about what they did with computers, these departments erected a uniform brick wall of secrecy.

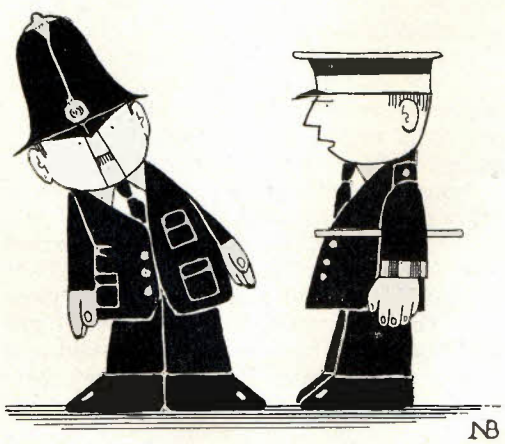
Penny a name

Two private companies — CCN systems of Nottingham, and the United Association for the Protection of Trade (UAPT) in Croydon — run Britain's largest computer databanks. Although credit references are the mainstay of UAPT's business (and a large part of CCN's), both companies spread their information business far wider. As well as receiving and passing on credit reference information, both companies have for more than five years used the Electoral Register — voters' lists — as the basis of computer databanks on the entire population.

This information is merged with many other databanks and sources of information. The Post Office's postcode system is used to index every address in the country. Every household in the country is classified into a range of socio-economic groups, ranging from inner-city/deprived/multi-ethnic to suburban/affluent, using data householders themselves supplied for the 1981 Census. Added to this are court judgements, and financial information about individuals and families from subscribers to the companies' services.

CCN have combined this information in a system called MOSAIC, which arranges for '40 million adults on the CCN database to be classified according to the area in which they live, combining financial, demographic, housing and Census data'. The system is 'designed to distinguish areas with different consumer preferences and characteristics'. The addresses are also linked to mailing lists of subscribers or customers that CCN's clients have provided, showing people's interests or purchases. Clients and subscribers get a discount if they feed in information as well as take it out.

Both CCN and UAPT have told journalists that they don't sell their information to private detectives and other snoopers. But they do. When *Secret Society* later filmed people looking at what was held on the CCN and UAPT databanks, we had registered to use their services in the name of a firm of private detectives.



'If there's one thing I detest, constable, it's a bent policeman'

CCN and UAPT buy lists of names on the Electoral Register from local councils for about a penny a name. Their computer checks cost from 50p to £1.20, depending on the information involved. There are 43 million names in CCN's 'Nationwide Consumer File', and the same number in UAPT's 'Infolink' service. A check on a given address will reveal, at a minimum, the names of all those over 18, or soon to be over 18, at a particular address. Each address is socio-economically coded, based on government Census data.

CCN call their system 'one of the most powerful tools around for the application of "cold" direct mail'. They will sell precise mailing lists of names and addresses, based on a sophisticated computer analysis of every household into families, single men, single women, and others. The age of all 17-20 year olds is also recorded. A CCN customer could thus order an address list of all 19-year-old single women living in a particular area.

CCN also offer a computerised debt collection system. From anywhere in the country, you can tell CCN's central computer that you're owed money and want it collected. But there's absolutely no check on the accuracy of this information. The computer will automatically harass someone without any check as to whether the debt was true in the first place. I tried the system out on myself — and, giving the address of the *New Statesman*, told CCN's central computer that I owed one of their clients £300.

There was no truth to this claim; I'd made it up that very minute. But I was soon threatened with court proceedings which would, CCN said, be instituted without further notice — unless I paid up within seven days. Written confirmation is only sought before a writ is actually issued — but even then, the client doesn't have to produce any evidence that the debt is real.

Public hostility

The BBC commissioned a special survey on public attitudes to private databanks: it found almost total public hostility. A standard sample of 1,000 people were asked in September 1986 what they thought of the information they gave when registering to vote being sold and used without their permission. Nearly eight out of ten — 79 per cent — disapproved or strongly disapproved of the sale of electoral lists. Only 7 per cent of the population *approved* of councils flogging off the voters' lists.

Gallup found even stronger hostility to UAPT and CCN having converted the lists into national computer databanks. Eighty-six per cent of the population disapproved or strongly disapproved of council voting rolls being sold to them — and most of the respondents (89 per cent) thought that the sale of voters lists to form a national computer databank should be made illegal. In other words, more than three out of every four people think that operations like CCN and UAPT should be outlawed.

But instead of legislating to protect privacy, the government has recently made protection more

difficult. Special new regulations, passed in 1985, now make it compulsory for the electoral register, if kept on computer by a local authority, to be supplied in the form of electronic data to anyone who wants it. Such data costs £15 per thousand names, or 1.5p per name. This change was introduced to help political parties who have started using micro-computers for canvassing at election times. But it helps commercial databanks even more. Previously, they had to order printed rolls and type all the information in them into the computer themselves, a lengthy and expensive process.

Since it is compulsory for all adults to register to vote, there is now no legal escape in Britain from being put on file by the private databanks. Only if you live in Greenwich — where the local council is the only one in Britain to refuse to sell electoral information for commercial purposes — can your privacy be protected. Greenwich protects its ratepayers by printing only enough copies of the electoral register for its own and political candidates' needs — and no more. Greenwich spokesman Jim Radford told us that 'it would be quite immoral to sell it to commercial companies'.

Activities like CCN's and UAPT's should therefore be a straightforward breach of the new Data Protection Act, which lays down mandatory 'Data Protection Principles', one of which is that:

> Personal data held for any purpose . . . shall not be used or disclosed in any manner incompatible with that purpose.

There is little compatibility between exercising a right to vote, and finding the information you gave cropping up in a national computer databank. But Data Protection Registrar Eric Howe says that CCN and UAPT can get away with using the electoral register this way because of a special loophole in the Act. This allows anyone to do anything with any information that is statutorily published — even if they violate the Principles of the Act itself. Howe did take up the issue with the Home Office. But the Home Office wasn't interested, and refused even a request from Howe that the Registration form be amended to include a warning about what would happen to the information. 'I'm disappointed', Mr Howe told us.

'The foundations for a standard government identity number for every citizen have been laid. The official number already has a name — the NINO'

Hey NINO no

In the public sector, the foundations for a standard government identity number for every citizen have been laid. The official number already has a name — the NINO, short for National Insurance Number. But the new title presages a far wider use for the old NI number than merely accessing national insurance records. All DHSS and Inland Revenue files are now being computerised, with each individual identified directly by their NINO. A DHSS Departmental Central Index, listing all of Britain's 54 million inhabitants, is being established at the department's Newcastle computer complex.

The Central Index isn't an official secret. But public discussion of the plan hasn't been encouraged either. Ten years ago, the Home Office-appointed committee on Data Protection warned of the dangers of establishing a universal reference number such as the NINO. They cautioned that the implications for privacy were so severe that 'legislation should be specially enacted' before a standard population identification number was allowed to evolve. Based on the experience of other countries, they feared that eventually people would be forced to quote any standardised number in any and all dealings with authorities.

This has now begun to happen. Local authorities have been urged by the DHSS to start recording NINOs for their tenants, in case they claim housing benefit. Credit card-like NINO 'Numbercards' have been issued to school-leavers over the last two years, and to young unemployed people. MI5, the Security Service, already use NINOs as their main reference number. And the entire DHSS index of names and NINOs has been transferred wholesale to the Inland Revenue.

The index taken from the DHSS is now at the core of the Inland Revenue's own new national computer system. Former Inland Revenue officer Tony Meredith told us about the result:

> The National Taxpayer Tracing System will be enormously powerful. It will find anyone within about . . . within a few seconds, from any one of 25,000 terminals in any one of 600 offices. ▷

He added that IR computerisation means that there will be 'very few controls' on why members of staff access information. So 'if someone within the Inland Revenue wants to pass information to an outsider, it will be very, very easy. They cannot be stopped.' Had he found people trying to gain access to Inland Revenue information? Meredith said:

> We have experienced people attempting to gain information from the Inland Revenue; I have been involved in a few, a very few exchanges of information with other government departments. The Inland Revenue tends to believe that it always gains more than it gives away.

Despite stern promises of confidentiality, Meredith found that the tax department was prepared to give personal information away.

To ensure that every tax payment reference is accompanied by the NINO, Inland Revenue staff have recently sent out letters asking taxpayers to provide their NI numbers 'to ensure that your contributions are properly recorded'. Challenged, they admitted that the real reason for asking for the number was to 'put [their own] records on the computer'. But Inland Revenue press officials have refused to discuss this or any other aspect of their computerisation schemes.

Computerisation of data is spreading across all of the public sector:

- In the National Health Service, computerisation now starts automatically with the Notification of Birth to each health authority. Information about new children is thus automatically put on computer, without necessarily informing parents that a record has been created.
- The Office of Population Census and Surveys has set up a secret computer experiment linking all the computer information available about a selected one per cent of Britain's population. Its so-called 'longitudinal survey' links data about selected traceable individuals, throughout their lives. The people included in this databank don't know they're there, or why. In fact, they have been selected on the basis of four secret birth dates. If one of these dates is your birthday, then you're in the system, and it will be following you around Britain and abroad, linking together information from all the other databanks.
- The 'Suspect Index' used by immigration officers will soon be on computer. There are 20,000 names on the Index, including drug traffickers and terrorists. But part of the Index is used to record the names of British subjects that the government would like to follow around.

According to journalist and former immigration officer Jolyon Jenkins (who himself worked on the *Secret Society* series), the British names on the index include Vanessa Redgrave, Tariq Ali, and Kim Philby. There were also at least two journalists on the index, Jenkins recalled, David Leigh of the *Observer* — and Duncan Campbell.

Next year, like the rest of the EEC, Britain plans to introduce machine-readable passports. Soon after, Chief Immigration Officer Peter Tomkins told a House of Commons committee last month, the Home Office will set up a nationwide computerised Suspect Index, with 500 terminals at ports and airports. The new-style machine readable passports are pushed into a special reader, and details logged, automatically, by the computers. Although the Home Office have been evasive about the value of machine readable *British* passports to Suspect Index (SI) checks, internal Home Office papers reveal their thinking that:

> One of the major benefits of an automated machine-readable passport system is the potential for performing automatic SI checks . . . an effective SI system can only be achieved through some form of automation.

The same official document explained that getting the new passports offered security authorities the chance to 'increase the capacity' of the Index, at the same time as creating an effective means of monitoring when and where selected Britains were travelling.

Ask a policeman

The most dramatic part of the *Secret Society* investigation of government databanks was the exposure of a network of unofficial information tappers. Since some of them may now face trial, the precise identities and whereabouts of their activities cannot presently be revealed. But our investigations began when one man with police connections ran an advertising campaign in the south of England for what he described as 'illegal' services.

I heard about this, and — disguised as a Glasgow businessman — arranged to meet him at a hotel near where he worked. Later, in the hotel's car park, a hidden camera secretly filmed him as he took money to pass on to 'mates' in the police force. I gave him a list of names of people whose personal police and DHSS files he said he could get.

He was told that the names were those of people seeking employment in a politically sensitive public company, which feared attempts at infiltration by political activists. The names he had been given were, in fact, all rather serious political activists. So information should have been available.

A second meeting was held at a riverside pub — where unknown to my informant, an entire BBC camera crew once again lay waiting, this time in the undergrowth on the far side of the river. His words were relayed to them by a radio microphone. He explained to me how easy it was to get official information:

> The chap that does my [criminal record checks] is just a beat bobby. He gets on the radio and says I've seen this lad doing this that and the other. Anything known about him? Punch it into the computer.

The information tapper also appreciated the value of having a single identity number like the NINO for getting information out of the system. He explained to me that in his job 'everybody's traceable by a National Insurance number'. It was very useful to him because 'tax and National Insurance and things like that . . . are all linked together'.

Some of his first checks were unsuccessful; but when he came back with accurate details of the criminal record of an animal rights activist in London, BBC Assistant Director General Alan Protheroe ruled that, as a *prima facie* offence had been committed, the police should immediately be given all the information so that they could take over the enquiry. A major police enquiry was launched, and is still under way.

Private detective Gary Murray, one of the people approached by the information tapper a year ago, told us that in his experience this kind of unauthorised leak was by no means isolated.

> I've been in practice privately for over 15 years, and I've had contact with literally hundreds of private detectives and security consultants. Since 1968, that I can recall, most of them have had access to official records.

IN SIX MONTHS' time, the new Data Protection Act will be in full force, allowing people a limited right to see what's held about them on computer. But government files concerned with law enforcement, prisons, or national security are exempt. So are any records held on (or recently transferred to) paper. Access fees will be high, and the limited amount of information provided about computer databanks and what they hold is so diffuse as to make successful searching for improperly held information almost impossible.

In any case, the Act lets people do what they like so long as they actually register whatever they intend to do. Industrial data specialist Ted Cluff, who runs the Institute of Data Processing Management, cheerfully acknowledged that 'the weakness of the Act is that provided you declare what you're going to do, you can do almost anything you like'.

The Act created the new office of Data Protection Registrar, whom the government at first proposed — ludicrously — should be a Home Office official. And, according to Sir Norman Lindop, who headed the official Data Protection Committee from 1976 to 1978, the Bill gave the Registrar hardly anything to do at all. 'It just said he may do this and he may do that', Lindop noted. 'One can imagine him sipping sherry on a Friday afternoon and deciding that he wouldn't bother.'

The Data Protection Act also deceives members of the public about who has access to computer data about them. Although the Register is supposed to list everyone who has access to the information on computers, police and security organisations can lawfully tap any databank — without leaving a record that they've been there. In this respect, the Act requires data users to tell lies. Lindop found this deplorable, and calls it 'a fraud on the public':

> I think it's most regrettable that an Act of Parliament should encourage people to think that they can use double standards and get away with it.

Unless it is is rapidly strengthened, the Data Protection Act is already too late and too powerless to stop private national databanks being set up, or to prevent identity numbers and official population registers creeping in 'by stealth' — as Sir Norman Lindop's committee recently feared. It's true that few government developments in computer databanks have been total official secrets. But Whitehall's attitude to the Secret Society *programme spoke volumes. Campaigners for privacy are forever asked what the innocent person has to fear. But what does the innocent Whitehall department have to fear from candour? What have they got to hide?* □

Secret Society *is being transmitted on BBC-2 at 10.20 on Wednesdays. Next week in the* New Statesman *and on BBC-2: war emergency planning.*