body, and finally hands were buzzed for traces of bomb-making material.

The security is there because of the IRA. Not a single one of Britain's political parties held a serious discussion on Northern Ireland at its national assembly although both Conservatives and Democrats considered political links between their parties and allies or affiliates in Ulster. It appeared on none of the conference papers at the SDP, which perhaps explains why David Owen made several off-the-cuff demands for the North to be enclosed in a fixed frontier of, presumably, concrete and barbed wire. International statespersons have to have something to say about Northern Ireland, not least because much of Europe and the USA seems better informed on the province than most Britons. This is partly because it seems simpler abroad. But also because on no other issue has the British media so singularly failed to keep the public informed.

This is not just the fault of British insularity. The larger blame falls on British governments, especially the Conservatives who have gone out of their way to terrorise British television into treating Northern Ireland politics in the same way that they do; viz varieties of murder. Last Sunday the government let it be known that it is considering legislation to enforce a ban on reporting the views of IRA members. Yet interviews with members of the IRA could have revealed the poverty of their political strategy several years ago. That would have given us something to talk about, such as what are the serious political and economic options for Northern Ireland if the IRA has nothing to offer? But such discussion does not fit a simple Tory view of killers and victims.

Mrs Thatcher, who made her ritual denunciation of terrorism and declared herself properly unmoved by their threats, would no doubt believe that such a discussion might be seen as a concession to terrorism. As Britain managed to ignore Northern Ireland before the resurgence of the IRA, so the show should go on as usual.

Yet the pretence that talking politics within a barricade is quite normal in a free society was in line with the rest of the conference. The mass refusal of Conservatives to acknowledge that there are any problems anywhere in the United Kingdom has given a perverse glimmer of hope to a few anti-Thatcherites. Such blinkered complacency, they reasoned, does not augur well for a party that needs to keep on top of things.

This is to play by Labour Party rules: that the state of the party is a guide to the actions of its leaders. It is also to assume that what leaders say at party conferences is an accurate guide to what they believe. Yet we know Mrs Thatcher is quite capable of inventing long-held convictions overnight, as on the environment. We know she is adept at "statecraft", we know she is quite capable of lying, as over Westland and Peter Wright, and misleading the public.

I cannot be the only person who saw in that Security Cordon round the Conservatives not just a defence against the IRA but also a powerful barrier of fantasy against political honesty. The danger for us all is that Security Cordon politics feeds the paranoia close to so many Tory hearts and, like Peter Wright, the ruling party becomes incapable of distinguishing the real dangers from the imagined. ●

The runaround

The Data Protection Act is virtually worthless. Duncan Campbell took four months and a stack of £10 notes to discover nothing he had not known

At the time, the cynics said that the 1984 Data Protection Act had nothing to do with personal privacy. The law was being provided only to protect commercial interests, which would lose out on lucrative international data processing traffic if Britain did not implement a national data protection law. Despite fine, resounding words in the act's "Data Protection Principles", they said, personal privacy would stay in the back seat. They were right. As a new report published by the National Council for Civil Liberties (NCCL) on Monday has emphasised, the new law has proved to be as relevant to personal privacy as the litter laws may be to the integrity of the ozone layer.

The final and most important provision of the Data Protection Act—Section 21, Subject Access—came into force on 11 November 1987. In principle, this section allows anyone to have access to any of their own personal data held on computer. In practice, it is subject to such wide exemptions as to be virtually useless. It is almost impossible to use effectively. I have tried to use this section, and have repeatedly questioned government departments about its effectiveness. Even obtaining the right form with which to make a subject access application could involve an interminable nightmare journey through the bureaucratic jungle.

Using the act is also punitively expensive; at a charge of £10 for every index you want to check (whether or not it holds any information about you), the exercise of personal privacy rights on computers are really only for the well off. That's no accident, either. Instead of allowing the Data Protection Registrar, Eric Howe, to set the suitable charge, the act left that key decision to government ministers. Last year, the Home Secretary Douglas Hurd, was repeatedly warned by organisations like the National Consumer Council and the NCCL that to set a charge higher than, say, a nominal £1 would frustrate the purposes of the act. Heeding this advice carefully, Hurd set the subject access fee at £10. Some data users (notably including the Home Office itself) have taken merciless advantage of the very high subject access fee repeatedly to charge applicants for checks of different files on the same computer system. A single subject access check can thus cost £50 or more.

The Data Protection Principles incorporated in (but hardly enforced by) the Act say that "personal data held for any purpose...shall not be used or disclosed in any manner incompatible with that purpose". But this principle is being violated millions of times a month by the biggest of the national data banks whose commercial operations contain files on over 40 million adults in Britain.

For many people the Data Protection Act has only eroded privacy. To date, many or most of the subject access enquiries to the Police National Computer (PNC) have been intended to breach applicants' privacy, by forcing them to obtain and hand over the contents of their criminal records entry (if any) when seeking new employment.

Prosecutions for violations have been few and far between. None has yet been for a case where individual rights have actually been damaged. This is not to say that such violations are not occurring. On the contrary, the villains are—as usual—getting away with it. Indeed (as explained below) the Act is such a labyrinthine absurdity that the chances of finding if an erroneous or damaging computer file on you might have resulted in refusal of a job, mortgage, loan, or security clearance are vanishingly small.

The ultimate verdict on the Act has been delivered by the people. It's not that people don't care about their privacy; it has been shown, in a dramatic series of opinion polls commissioned successively by the BBC, the Data Protection Registrar, and the National Consumer Council, that most Britons object strongly to commercial and other organisations trafficking in private, personal data, and want this made illegal. But, according to figures provided to enquiring MPs, the public are not sufficiently bothered to find out what's in store about them. After trying to use the Act, I can see why.

At the start of April 1988, anticipating speedy results, I set out to determine how easy it would be for ordinary people to find out if a particular computer contained information about them. For these purposes I decided to check the PNC. This database should have revealed an ample pile of adverse commentary on me.

The search was a debilitating affair. It took visits to three libraries, three police stations, and a host of lengthy telephone calls to government and other departments even to establish to which person or office a request for subject access to the PNC should be directed. More than four months had elapsed by the time I had the answer to the last of my subject access enquiries—and this said that since they didn't think they would find anything, they were not going to bother searching anyway!

The first phone call was to the Data Protection Registry in Wilmslow, Cheshire, for advice. Easy, they said, write to the Police National Computer Unit (PNCU) in Dean Ryle Street,

London SW1. But to find out what databanks existed and could be checked on the PNC and other computers, I would first have to consult the Data Protection Register. The Register was "easy" to find in any large public library.

After several difficult and unsuccessful forays to find the Register, another kindly soul from Wilmslow informed me that they would send a list of where the Register was held. This took a month to arrive, by which time I'd found by other means that a remote library in Wood Green did indeed hold the Register.

Wood Green's librarian was sure that the Register was an item no one else had ever wanted to see. Might one nevertheless look up the PNC? Blank stares met inquiring eyes, so the initials were explained. Brows now furrowed, body language clearly conveying a strong impression that my newly-disclosed purpose was self-evidently treasonable, perhaps worse. His view seemed to be that merely to wish to find out whether one could check one's record on the Police National Computer might—or, probably, should—itself constitute a criminal offence meriting inclusion on the aforementioned.

The microfiche stated specifically that all subject access requests should be sent to the Data Protection Officer at the Police National Computer Unit in Dean Ryle Street. But he never replied. Instead, a quite different Home Office department asserted that "it is not possible for the Home Office to assist you in this matter since it is neccessary for an applicant seeking information held on the PNC to submit their application through their local police force".

But the Data Protection Registrar had given quite specific information about how and where to apply. Another call to Wilmslow—was their magnificent Register wrong, or were the police and Home Office giving me the run-around? "Yes...and no", said the answering mandarinette, unimaginatively basing her best lines on *Yes Minister*'s Sir Humphrey Appleby. I might find this run-around tiresome, she said, but "it was just the way that the police went about things".

The exercise of personal privacy rights on computers are really only for the well off

(Perhaps we should not be too shocked by this Whitehall-like behaviour; the Data Protection Registry won the 1985 "Golden Bull" award for the most incomprehensible official prose of the year from the Plain English campaign and the National Consumer Council.)

The local police station now told me that forms could not be sent by post. Please come round in person—whereupon, after the inevitable lengthy wait in line with lost parrot and cat owners and the other sundry occupants of a smoke-filled police station waiting room, I learned that this "local" police station didn't feel quite local enough even to hand over a blank form. Eventually, a full six weeks having passed, I found a police station which would yield the application form, on pleasant pink paper.

"Application Form A" is notable for the fact that it attempts to persuade the enquirer to hand over more new information to the police than they already have. (Viz, describe any "incident" in which you were involved which we might (or might not yet) know about. Give full details, including anybody else involved.) No one could accuse the Met of not meeting the challenge of the Data Protection Act imaginatively.

Or of failing to do their best to run the police on sound commercial lines. According to Application Form A, fully to check the Police National Computer alone would cost £50. To check all Metropolitan Police or Home Office computers might cost £250. To check every police computer in the country would cost well over £1000. And there were, sadly, no discounts for regular customers of police services. So, it was back to the "local" police station, to hand over five crisp brownies with the completed Application Form A.

After another 40 days (the maximum statutory time for a reply), the PNC dossier finally arrived from the National Identification Bureau (a little known inter-police agency, based in Croydon). Campbell, Duncan/Wilson/Archibald was indeed recorded, having "first come to notice" while at Oxford University in 1972, aged 19. Reference number 73409/72L. Sex was male, height 5'11" (the most offensive part of the record to an aspiring six foot tall male), and [skin] colour, for some reason "unknown". "No cross references held", it said reassuringly, adding that there was "no convictions record on the Police National Computer". Nor was there a special "Crime Pattern Analysis" of one's preferred styles of crime. There was, however, a set of ten digitally reproduced fingerprints, each with their accompanying computer codes.

But the report refused any details of whether or not this individual was the subject of any "warning signs", special "flags", personal "wanted/missing" or "suspect vehicle index" entries on the PNC. The accompanying letter said that if no information was given, then either there was no information stored anyway or that there was "no information which [we are] required to give you under the terms of the Act".

They weren't going to say which of these two arguments applied. Unlike the US Freedom of Information Acts, therefore, a DPA enquiry will not tell you that there is a special file on you, even if all the information in it is kept secret. But it is the very fact of the existence of these recondite little entries on the PNC which most jeopardises civil liberty. The hidden fields can and do sometimes say that someone is a drugs user; or violent; or homosexual; or "of interest to Special Branch"; or that although the person concerned is neither wanted, missing, nor a criminal, her or his whereabouts should be reported to some other government department. (All these things have been found to have been secretly recorded in the past.)

My long search ended early in August with the receipt of a final letter from the National Identification Bureau. I would be getting £10 of my £50 back, it said, since the Bureau had decided not to bother to search the PNC Message Log after all, as they didn't think they would find anything. It scarcely seemed worthwhile to write back saying "Please try harder".

Almost all the takeup of the new data protection rights, it turns out, came from civil servants

With Labour MP Chris Smith, I tested whether, after six months, anyone was actually bothering to use the Act to check up on their government records. But apart from the Ministry of Defence (which had enthusiastically and actively encouraged service personnel to check on their own records) and three other departments with similar policies, most of the great British public had not taken any notice. We asked each government department how often between November 1987 and May 1988 they had been asked to check their computer records under the DPA.

Almost all the takeup of the new data protection rights, it turns out, came from civil servants. The only organisations which received any public enquiries—and were making money out of the applicants—were, predictably, the police and the Home Office. Even then, the enquiry rates were extremely small. Of just under 5000 requests, less than 150 appeared to have originated with members of the public. Most of these went to the Metropolitan Police (121) or the Home Office (21).

In the future, we face not just Poll Tax Registers and increasing commercial databank development, but a whole range of new government projects. A contract for the £300 million Government Data Network (GDN), for example, was announced in May this year, and will provide data links within and between such major departments as Health, Social Security and the Home Office. Until May, too, the government had deliberately lied about whether or not the PNC would be part of the new Government Data Network. It will be; indeed only last week the Home Secretary revealed for the first time the hitherto secret plans for an additional "Police National Network", linking every major police computer system together.

The lie about the PNC depended on not pointing out to Parliament that while the current PNC computers would be scrapped and replaced, and therefore would not be connected to GDN, the new PNC system known as PNC2 had always been planned to be connected to the government network. Whitehall dishonesty like this makes stringent outside supervision of government handling of personal data imperative. ●

Additional research by Lyn Barlow