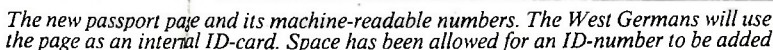


## Steve Connor

The history of the machine-readable passport begins at a meeting in Montreal in May 1968 held under the auspices of the International Civil Aviation Organisation (ICAO). This body, which represents the world's civil aviation authorities, was concerned with the dramatic increase in passenger numbers, during the previous decade, and the likely increase in the future. With machine-readable passports, it was thought, people could pass through airports faster. The ICAO set up a panel of experts to investigate the problem. The experts were drawn from Australia, France, Canada, West Germany, India, Kenya, the US and Sweden. Later on, they were joined by the USSR, Britain, Belgium and the



The new passport page and its machine-readable numbers. The West Germans will use the page as an internal ID-card. Space has been allowed for an ID-number to be added



Netherlands. Everyone, it was said, could benefit from shorter queues at the immigration desk.

Between 1969 and 1978, the panel held five meetings which set out the technical specifications that each country should follow if it wanted to adopt a machine-readable passport. The meetings were monitored by the International Criminal Police Organisation—Interpol—not because it, too, was interested in shorter queues at airports, but because the new passports could help the security checking that is performed at the world's various ports of entry. Interpol represented, and reported back to, the police in the countries concerned. The ICAO's panel recommended what the new passport should look like, what information the machine-readable zone should contain, and what the security considerations should be.

The print on the plastic laminated card must, for example, be able to withstand temperatures ranging from  $-10^{\circ}\text{C}$  to  $+50^{\circ}\text{C}$  without loss of quality. The document should be able to withstand even greater differences in temperature, and should not lose its reliability when stored at relative humidities of 0 to 100 per cent.

More importantly, the panel decided on the standard print to be used in the machine-readable zone at the edge of the page. The panel formulated rules for the dimensions of this zone, and the information that it should include. In this way, the new passports can be read by the appropriate machine whether in Manchester, Munich, Moscow or Miami.

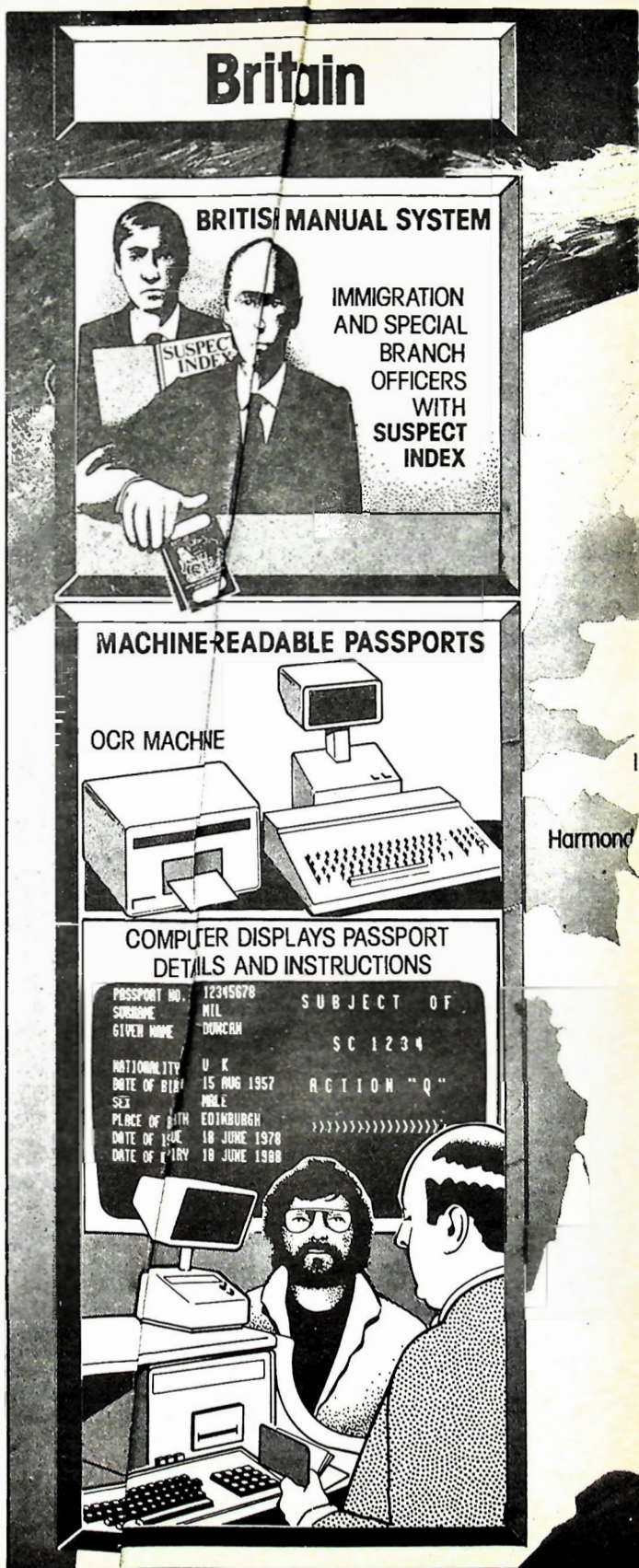
The machine-readable zone consists of two lines. The page itself is inserted into the passport and the zone becomes the outer edge. The upper line carries the letter "P" to indicate that it is machine-readable, the code of the issuing state and the name of the bearer. The lower line has the passport number, nationality, date of birth, sex, date of expiry, and a national identification number (which is optional). The date of birth, passport and national ID numbers have a "check digit" at the end of each. This number is calculated using formulae (Box B) and is a way of checking that the machine has read the line of characters correctly and that the number in question is valid. At the end of the lower line is a final check digit which, applying the formulae to all the numbers in the line, acts as a final check.

The digits also make forgeries more difficult—but not impossible. If the plastics laminate is broken, a chemical reaction takes place involving atmospheric oxygen; the paper darkens, making it clear that it has been tampered with. This can be done by impregnating the card with the reduced form of a dye. When it comes into contact with air, it oxidises and darkens. When the ICAO considered these security precautions, it had no illusions about how effective they would be in stopping forgeries; it clearly thought that it would just discourage counterfeiters by making forgery unattractive to potential criminals.

The ICAO's job was done. It had designed the standard machine-readable passport that suited all the countries involved; it even considered what the British Home Office was later to describe as the "Big Brother" aspect. Instead of having a machine-readable zone that people could not read (a magnetic strip, for instance, like that which appears on banking cards), the ICAO agreed that the zone should have roman letters and arabic numerals able to be read by optical character recognition. So the logic goes; no one has anything to fear that the machine-readable passport carries information they know nothing about.

In fact this is a sop. The machine-readable passport is meant primarily to prove the identity of the bearer. But few people understand that it will also give the immigration officer access to a computerised file that corresponds to the name carried on the passport.

*The Council of Europe wants a security network based on the INPOL computer at Wiesbaden (right). The Home Office has discussed a UK network to help immigration control*

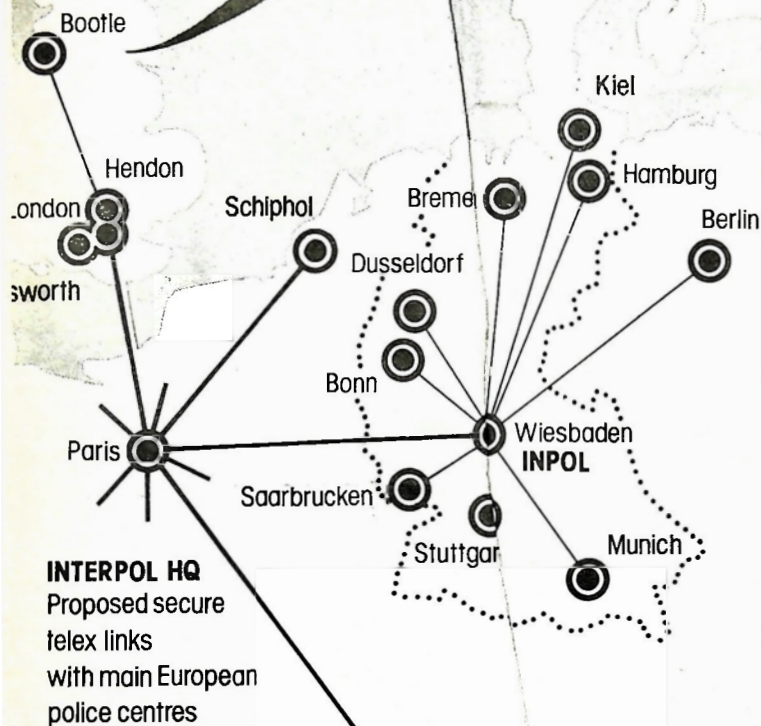




# West Germany

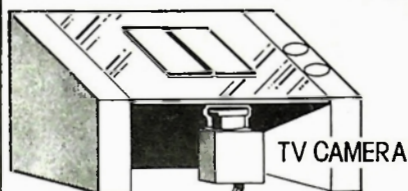
Bootle	- National immigration computer
Hendon	- National police computer
Harmondsworth	- Immigration service intelligence computer
London	- M15 computer

**EXEMPT FROM DATA PROTECTION BILL**

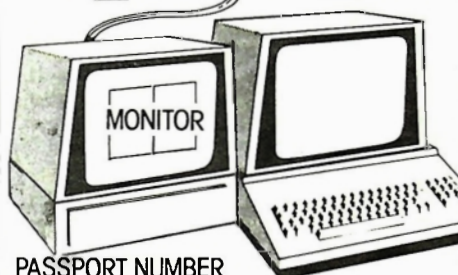


## CURRENT SYSTEM

PASSPORT FACE DOWN ON GLASS

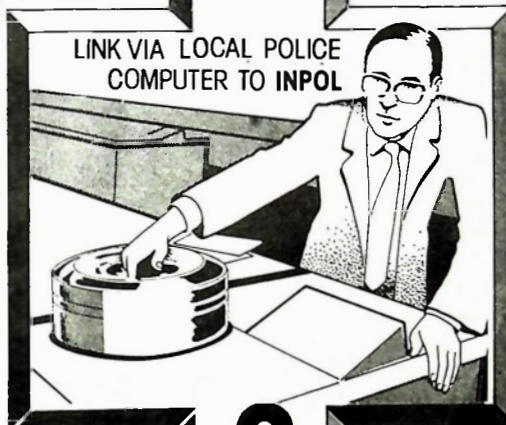


TV CAMERA



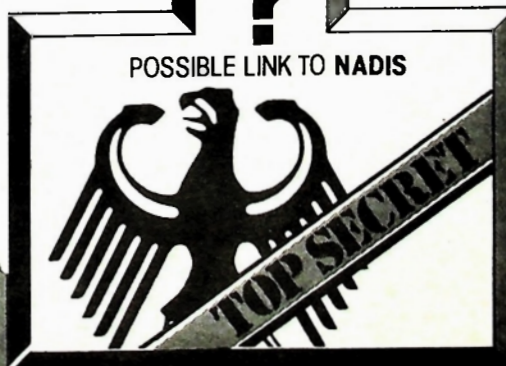
PASSPORT NUMBER TYPED INTO COMPUTER

LINK VIA LOCAL POLICE COMPUTER TO INPOL



?

POSSIBLE LINK TO NADIS





It is the information on this computer that is important in terms of the "Big Brother" aspect—the British Home Office, for one, has no intention of giving anyone but itself access to this information.

At the point where the passport is inserted in the reading machine—the interface—the ICAO relinquishes its responsibility. From then on, the machinations of security are under the control of the country in question. The ICAO sums up the implication of its decisions more diplomatically: "The requirements will differ considerably from country to country. For example, some countries may wish to record the inward and outward movements of all categories of travellers; some countries may wish to record the inward and outward movements of some categories only; and others may be concerned only with partial controls for specific groups."

In Britain, the imminent arrival of the machine-readable passport caused a great deal of interest in a Home Office group looking into a different task. This group examined ways of improving the suspect index—a list of people who, one way or another, have aroused the interest of the immigration authorities. By 1980, the Home Office had decided to amalgamate the suspect index with the plan to introduce machine-readable passports. As one of its internal documents states: "One of the major benefits of an automated machine-readable passport system is the potential for performing automatic checks on the suspect index."

The current suspect index is a classified document, and its "confidential" status means it must be kept under lock and key when not in use. For the time being, the index is a list of 18 000 names in the form of a black, A4-sized book. It is this book that international travellers can sometimes see in the hands of an immigration officer standing behind the immigration desk and looking at the queue that forms in front.

The Home Office is highly secretive about how people end up on its suspect index, and the categories into which they are put. In fact, the names are supplied by the Home Office, the police, the Foreign Office, the security services (MI5), Customs and Excise, and Interpol. Next to each name on the list is a coded letter: "X", for instance, means refuse entry; "A", "AA", and "J" are categories of interest to MI5. People in these categories are either stopped and questioned by special branch officers, who are always present at immigration control, or they are allowed to pass through and the border crossing is noted for the police or MI5.

The problem of having a list on paper is that it is difficult

to add names and take them off. With a computerised list, changes can be made at the touch of a button. Computers also mean that a greater number of people can be made "suspects". At the moment, 18 000 names is about the maximum that can be handled in a book. With a computer file, the Home Office can expand this number considerably, and it shows every sign of doing so. One internal report states that if demand to increase the index were met, it would double within two years. Another separate report, shown to *New Scientist*, states that putting the suspect index on computer will "assist the immigration officer in obtaining very fast and effective checks against a much larger suspect index" (emphasis added). This contrasts with the Home Office's public utterances that there are no plans to expand the suspect index.

### European data network

The Home Office says that the suspect index is a list of people "subject to immigration control". There is no doubt that some are criminals and terrorists. A clue as to how wide the index spreads comes from secret categories of international travellers of particular interest to MI5. These include: "Passengers who have been in a communist country . . . passengers in possession of communist or other subversive literature or who carry a CP card . . . [and] . . . passengers of Chinese race known or suspected to be travelling to and from the People's Republic of China."

An interest in people carrying "subversive literature" is not unique to Britain. In West Germany, such an interest is widespread. The West German border police, for instance, are issued with a list of "left influenced" magazines to help them distinguish between "suspicious" and "non-suspicious" reading material. Cooperation between West European countries to exchange information about suspected terrorists and criminals is a recurring theme within the Council of Europe. In a report on terrorism in Europe, the council states that "an essential requirement for controlling terrorism is a sophisticated intelligence-gathering system". And an integral part of this is tighter passport checks "however repugnant this may sound to those for whom European cooperation means making frontiers less and less relevant".

The council singled out the West German police computer at Wiesbaden as having made a significant "breakthrough" in tracing terrorists at home and abroad. This computer, which has 10 million "items" in its data bank, is run by the Federal Office of Criminal Investigation (Bundeskriminalamt) or

### A: How optical character recognition works

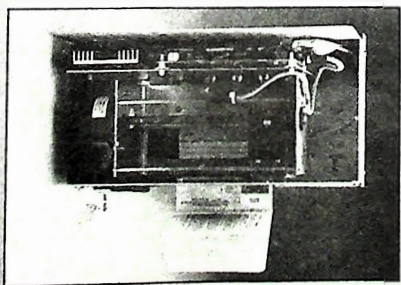
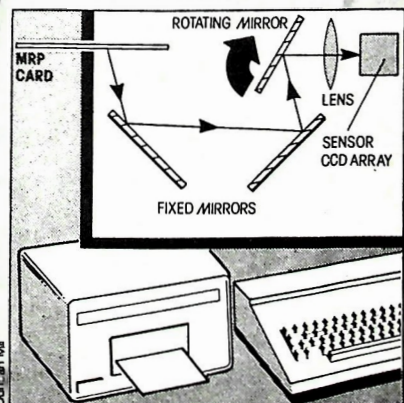
THE machine-readable zone of the passport is inserted into the reading device. This activates a micro switch and the card is gently gripped between rubber blocks to prevent any movement that could distort the reading of the zone. A light inside the device illuminates the two lines of the zone in a uniform manner, and a rotating mirror

reflects the images onto a photosensitive detector that compares the character being read with characters in its memory. If the two coincide then the character in question is read successfully. The device under test have a reading speed of about 100 characters a second, and the aim is to have an error rate of less than one part in 10 000.

As the zone is read, the check sums are calculated, the details on the passport are flashed to a computer screen, and the identifying elements—birth date, name, passport number and identity number—are sent to a computer where they are checked against the list of names in the suspect index.

The chevrons in the machine-readable zone are for blank fields. In the West German ID-card/passport, part of it is taken up by the national ID-number. On British passports this is left blank, although the devices being tested by the Home Office can read passports with ID numbers on

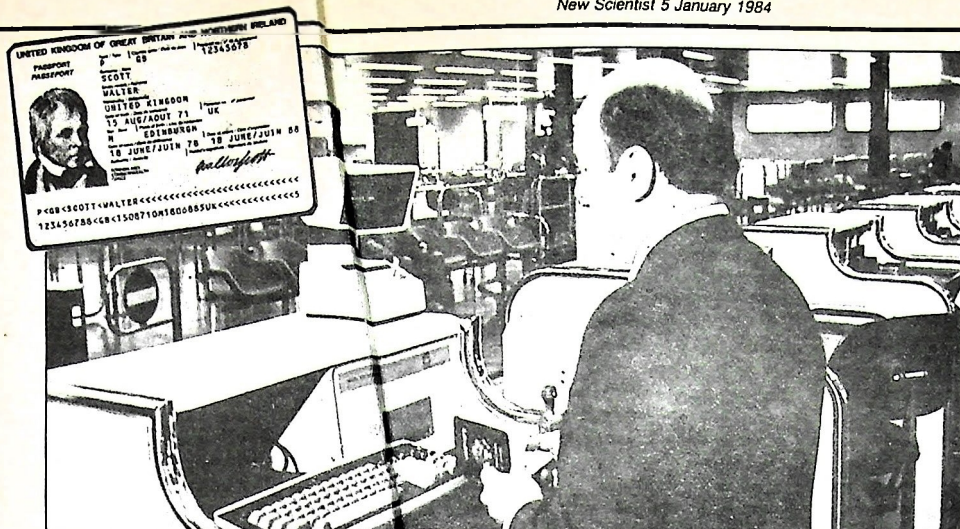
them. The Home Office has already tested two of these machines at Heathrow airport and will test more this year. □



Mechanics of an OCR machine . . .

. . . the principle involved





The first immigration desk for the new passports opened at Heathrow last April; the machines read 90 per cent of the new American passports successfully; inset is a sample page

KA). This federal computer—called INPOL—is linked to the computers of each of West Germany's 11 regional police forces. Each regional force is in turn linked, via the INPOL machine, to three other computers: the central registry of aliens at Cologne, the central registry of vehicles at Flensburg and the central registry of criminals at Berlin.

West Germany also intends to introduce machine-readable internal identification cards that every West German must, by law, possess. The ID-card will be in the same format as the passport envisaged by the ICAO; West Germans will also be able to use them as passports within the European Community (EC). When travelling outside the EC they will be encouraged to carry both passport and ID-card.

West Germany automated the task of checking travellers entering the country some years ago. At Berlin's Tegel airport, for example, each passport control point is fitted with a glass plate, conveniently out of sight of the passengers. A TV camera lies underneath. When the passport is put on the plate face down, the camera relays a picture to a person operating a computer terminal in another part of the airport. The computer is connected, on line, to the local police computer, which is in turn connected to the central INPOL computer in Wiesbaden. As the operator keys in the passport number that appears on the TV screen, the computer can give an almost instantaneous indication of the wanted status of the traveller. The operator conveys this to the immigration official by illuminating an appropriate coloured light at the official's desk or by telephone. During March 1976, immigration officers at Tegel airport interrogated the computer 56 832 times and had 172 "hits"—a success rate of 0.3 per cent. Foreigners' passports are also checked.

West Germany plans to perform similar checks on the movements of people across its borders, but this time with machine-readable passports and identity documents. Initially 40 OCR devices will be installed at airports and motorway borders; by the end of the decade the figure will reach 400. At present, using the system similar to the one in Berlin, only 3 per cent of all West Germans leaving or entering the country are checked. By the end of the decade this could, in theory, rise to nearly 100 per cent. By 1989 the number of machine-readable ID-cards in West Germany will reach 40 million.

Today, the West German police can stop people under a variety of circumstances and ask to see their cards. In the future, internal checking will be possible on a scale similar to that planned for airports and borders. The OCR devices themselves are relatively light and mobile; they could be set up by police at roadblocks to check who is entering or leaving

a particular area. This happens already. During some demonstrations, for instance, the police have taken down the numbers on the ID-cards of people on buses and trains that are heading towards the protest.

The INPOL computer contains a list of wanted persons, just as there is a list of wanted persons on the British Police National Computer (PNC). One of the sub-categories on INPOL's wanted persons' file is BEFA 7K (Beobachtende Fahndung or observation search). A BEFA 7K person, according to one border control officer, is one who "is found somewhere with a BEFA 7 person [suspected terrorist], that is with an actual suspect even if it is purely accidental,

whether it be in a train compartment, in a sleeping car or touring bus". Another category in this file is BEFA 9: participants in demonstrations.

There is little doubt that information about BEFA 7K and BEFA 9 people goes to and from the West German security service computer, NADIS. This computer is run by the Verfassungsschutz-Behörde—the Constitution Protection

## B: Calculating check digits

THE machine-readable passport "contains only information that can be read with the naked eye", says the Home Office. This is true. But within the lower line of the machine-readable zone are numbers called check digits. They are not immediately recognisable because they appear at the end of another number that has some relevance—date of birth, passport number or date of the passport's expiry. The check digits are calculated using a set of standard rules. The value of each digit depends on the number it follows. The rules have four steps:

**Step one** multiply each digit in the original number (such as date of birth) by chosen numbers called weightings. The weightings chosen for machine-readable passports is the series 731731731....

**Step two** add the products of these multiplications.

**Step three** divide the sum by a chosen number, known as the modulus. It is agreed that each country should use modulus 10.

**Step four** specify the remainder of this division as the check digit.

And so, using the date of birth of 1 November 1955 as the example. The date of birth becomes 011155. But problems can arise as to the order of day, month and year. The US method is to put month first so this date becomes 110155. And to complicate issues further the International Standards Organisation puts year first, so the date becomes 551101. We shall use the normal, British format for our example.

<b>Step one</b>	
original number	0 1 1 1 5 5
weightings	7 3 1 7 3 1
products	0 3 1 7 15 5
<b>Step two</b>	0+3+1+7+15+5=31
<b>Step three</b>	31÷10=3, remainder 1
<b>Step four</b>	check digit is 1.

The number appears on the passport as 0111551. Similar calculations are done for passport number, date of expiry and (in some countries) national identification number. A final check digit is calculated using all the numbers in the lower line of the zone, and this digit appears at the very end of the line. The machine that reads the zone performs these calculations almost instantaneously and it is a way of checking that it has "read" the zone correctly. It is also a way of ensuring that the passport is bona fide and follows the rules. □



## West Germany provides financial role for ID-card

**WEST** GERMANS are legally obliged to possess identity cards. The West German police have virtually total freedom to check the card of anyone in a public place. Anyone not carrying one may be held until they can identify themselves. The new, machine-readable cards (MRCs)—identical to the laminated page in the EC's machine-readable passport—will help the police make even more thorough checks. MRCs will also come to the aid of private business. The law introducing them includes "expressis verbis" permission for banks, insurance companies, building societies and the like to use MRCs. The owner has to agree to this private use which must exclude the serial number on the ID-card.

All West Germans must register their home address with their local councils; a requirement that, added to the need to carry an ID-card, enables the police to check anyone very carefully. The police are not allowed to ask to see the card of anyone who is at home without "reasonable suspicion", but it is easy for a police officer to be suspicious.

Identity checks increase after terrorist attacks or a bank robbery. MRCs will allow internal checks to increase several times over.

Both the private and public use of MRCs are the subject of fervent debate in West Germany. The law is explicit about the use of card serial-numbers to file private data. The government printer in Berlin that prints the cards must destroy its record of which serial number is issued to which card. The number may be used only by the police and local councils. This safeguard was introduced after a decision by the Constitutional Law Court in Karlsruhe two years ago.

However, companies may add their own serial numbers to the data on the MRC. The card is fed into a reading machine, an account number, say, is added to the information and the company is free to use the card for identification or anything else. A

bank, for example, might ask all customers to produce their MRCs. It could then survey customer habits to help it decide how much money to hold, when to put on extra counter staff and when to take them off.

The private use of MRCs is particularly subject to heavy criticism. Hans Peter Bull is professor of jurisprudence at the University of Hamburg and the past government watchdog on the misuse of electronic data by the administration. He said: "It is absolutely necessary to exclude any private misuse of such a sophisticated control technology. The arguments concerning voluntary use are misleading, because people will be forced to present their ID-cards when they need to use the services of companies. And there will be no other choice when every company has decided to use the ID-card for identification."

Dr Herman Schnoor, minister of the interior for the State of North-Rhine Westphalia, shares Bull's concern: "The protection of individual rights works quite effectively within governmental administration. But there is a gap in the control of private-sector data processing. The government's data-protection watchdogs cannot get their hands on privately held data. We should be very careful with the extension of the use of ID-cards in the private sector."

Federal and national laws protect West Germans against the misuse of personal data held by government agencies. Independent watchdogs can check the daily collection, storage, processing and transferring of data within government departments. Annual reports are published on data misuse, and offenders face fines or even imprisonment.

The debate over MRCs grew out of a controversy last year concerning a detailed population census. Citizens were to be asked some very personal questions, concerning income for example. Some questions were so personal that even the most law-abiding Germans rebelled against it. Public discussion about the census sensi-

tised public opinion to data protection and civil rights and that sensitivity is now concerned with the MRC.

One of the most criticised features of the new MRC is that the police could store massive amounts of data about people under surveillance. Even the fact that an individual has been asked to produce their card is added to the INPOL computer file—a practice that allows the police to check any person's movements.

That such a large amount of data can be stored is probably the weakest point of the new law: it includes no mention of the circumstances under which such data should be stored. Nor does the law cover cooperation between police forces and the Constitution Protection Agency (Verfassungsschutz-Behörde), which is roughly equivalent to MI5 in Britain. Every federal government and the national government has such an agency to monitor the activities of political extremists and terrorists. The police and the agencies have a large degree of freedom as to whom to include as being under "police observation". A spokesman of the Hamburg agency told *Der Spiegel* in August that the number of people under "police observation" had increased by 50 per cent since early 1982. He claimed that up to 11 000 people can be put under observation after a terrorist attack.

Most of the critics are not arguing against the technology. But they do want sophisticated control mechanisms to be built into the law and these to be accompanied by specific civil rights regulations to prevent the misuse of data. Bull adds another argument: "As the police's capacity to control has grown so large the legal base for cooperation between the West German intelligence service (Bundesnachrichtendienst) and the constitution protection agencies should be clearly defined. This is not yet the case, and it should be done before the new ID-card system is introduced."

**Rolf Zell**

Rolf Zell is a freelance journalist working in Stuttgart.

Agency. As with MI5's top-secret computer, in London's Mayfair, little information is available about NADIS.

The picture emerging from West Germany is one where information on people's movements within and outside the country is monitored by a series of interlinked computers. The central police computer, INPOL, is linked to the regional police computers, and to the three central, national registries. And between INPOL and NADIS, information about the movements of people flows quite freely, even though there might not yet be a direct computer-to-computer link. It is for this reason that the Council of Europe holds up the INPOL computer at Wiesbaden as the example which other European states should follow.

The council is backing a plan to set up a Europe-wide computer network with the Wiesbaden computer at the centre. The network is to "exchange topical information on the daily situation with special regard to transfrontier movements of members of terrorist circles . . . and to establish secure telex lines between national police centres". At the centre of this vast surveillance network is the machine-readable passport—a document that the Home Office says will help shorten queues at the arrivals desk of immigration control.

But even the council cannot ignore the risks that machine-readable passports pose: "The question . . . is how far a state can go to improve security without dismantling freedoms which once gone may never be regained. . . . And how can we make sure that legislation designed to combat violent terrorism is not abusively applied to repress radical, but non-violent, opinions or political forces?"

In Britain, the linking of state-run computers is not as advanced as in West Germany. But nevertheless, the Home Office is considering connecting the passport computers holding the suspect index, at air and sea ports, to its national immigration computer in Bootle, Merseyside. This link could do away with the landing and embarkation cards that now have to be filled in by hand by people wishing to stay in Britain. Internal documents show that the Home Office has discussed a national network of computer systems to help immigration control. And there are other computers that store information of use to immigration officers sitting next to their computer terminals. There is information on the PNC in Hadon, there is information on the immigration services' intelligence computer in Harmondsworth near Heathrow, and, most secret of all, there is the information on MI5's computer, sitting in the heart of London. □