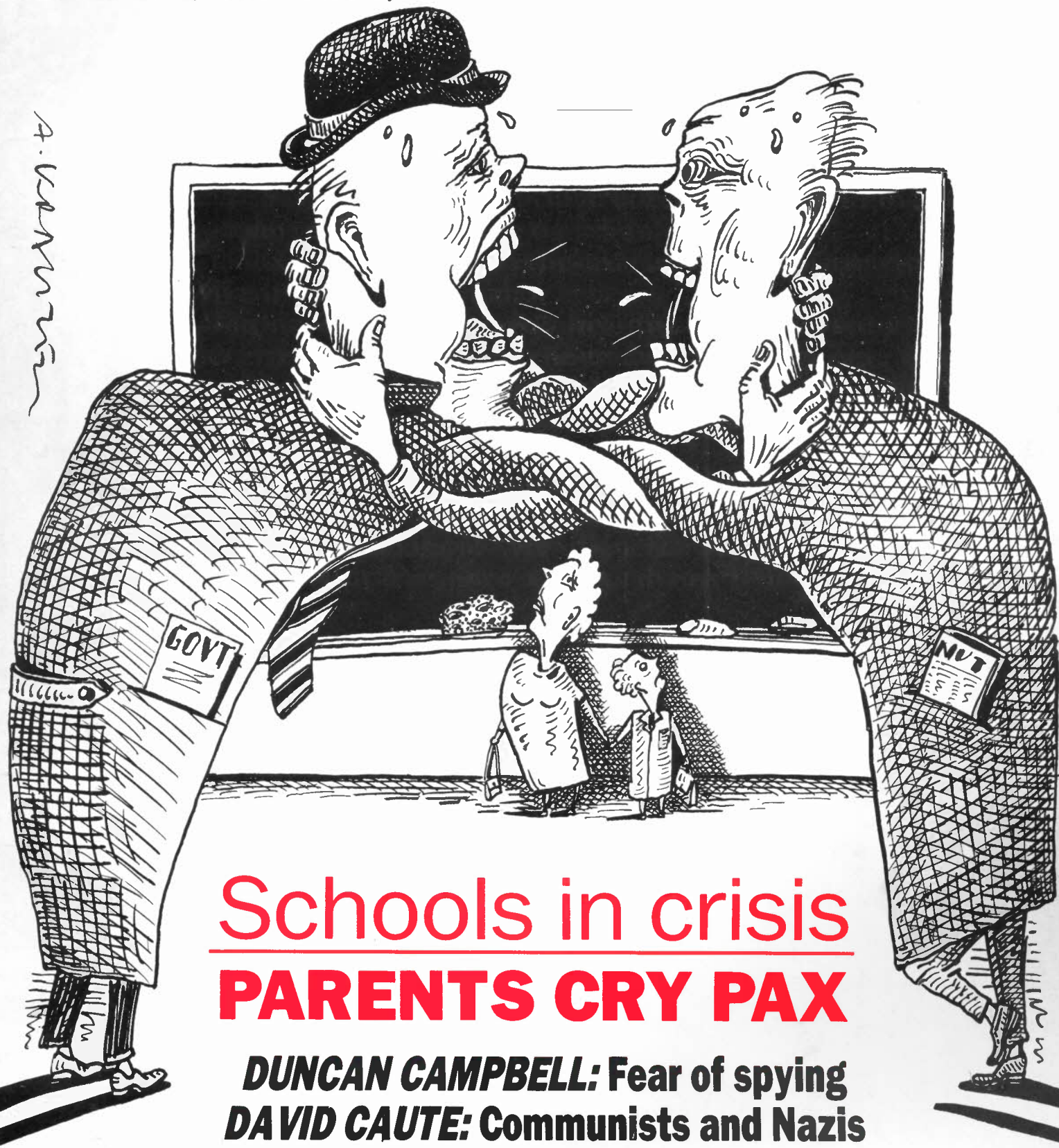


New Statesman

24 January 1986 80p IR£1.28 US\$1.50 By Air

I ♥
AMERICAN
FOOTBALL



Schools in crisis **PARENTS CRY PAX**

DUNCAN CAMPBELL: Fear of spying
DAVID CAUTE: Communists and Nazis

THEY HAVE BEEN watching me. For at least seven of the last nine years, they have tapped my telephone. Sometimes, they followed me around. And I am not paranoid. They really were out to get me, if they could. I am of interest to surveillance organisations as a journalist who investigates technology and its role in military or intelligence matters. But many other people also fear their phone might be tapped, their mail opened, their movements followed.

At first, my answers to these anxieties seem comforting. Almost nobody's phone is tapped. Ask yourself how much it would cost every week to record, transcribe, examine, read and take appropriate action over the average person's calls. And even then, what value does tapping have? In seven years' tapping of my own phone, nothing was accomplished except to make me angry, not afraid.

Almost nobody is watched. Think how much it costs to train, employ and equip the necessary dozen or more people needed for the full time physical surveillance of one person. Remember to allow for overtime payments, sick pay, national insurance . . . and luncheon vouchers. Even the secret police have to eat.

Even when the secret police are not at lunch, their efforts can rival the Keystone Cops. I was once tailed round London by a convoy of identical brown Hillman Hunters — with identical members of the brown raincoat brigade inside. Of course we aren't being watched full time. And even if it sometimes happens, there may very well be no result.

But many people are certainly scared that the watchers and listeners are out there, unseen. What they experience is the 'chilling effect' of government behaviour. One woman who has felt that cold breath wrote to ask: 'Why should I be watched? I've never been involved in crime or politics.'

This is a 'democratic society'; yet she equates politics with crime. Lots of people do — and they are, as a result, very much afraid to exercise their rights as citizens.

In the United States, the Supreme Court has brought many judgments on the 'chilling effect'. They explain it this way: If the conduct of government and other public agencies is such that the ordinary person may have cause to fear the intrusion of officials in the course of the lawful exercise of individual rights and human liberties, then that government behaviour has an unlawful 'chilling effect' on freedom.

Surveillance technology intensifies the 'chilling effect'. With advanced, sophisticated technology, a totalitarian or authoritarian state may try to determine and

THE CHILLING EFFECT

Paranoia is a potent political force. When it is a fear of government surveillance it can paralyse democracy. That fear may focus on the wrong objects but, argues DUNCAN CAMPBELL, it is not without reason

control efficiently the ways that its subjects are permitted to think and act.

At present rapid progress is being made in the ability of computers to 'comprehend' speech and recognise visual images. When these developments become more sophisticated, computers will be able automatically to transcribe and, to a limited extent, interpret human speech. Telephone tapping could then become a widespread, completely automatic process.

Visual recognition techniques are also developing fast. The first glimmering of tomorrow's technologies of this kind include computerised scanners. They have already been tried out on three British motorways. The scanner computers automatically read vehicle number plates, and flash a warning signal if the vehicle is of interest of police.

Giant computer databanks necessarily play a central role in the demonology of Big Brother technology. This is not without good reason. The power that computers have to bring together information, then sort and collate it has been growing exponentially for three decades. It will continue to grow.

ONE REMARKABLE system of recording information about the population at large is being developed fast but with no accompanying publicity. Since 1966, all police forces have been asked to appoint Local Intelligence Officers usually inside major police stations. These Local Intelligence Officers — sometimes called 'collators' — are required to assemble a 'memory databank' on anyone and everything in their area. Individual area constables — nowadays they're called

'community police' — are required, as their first duty, to feed information to the databanks.

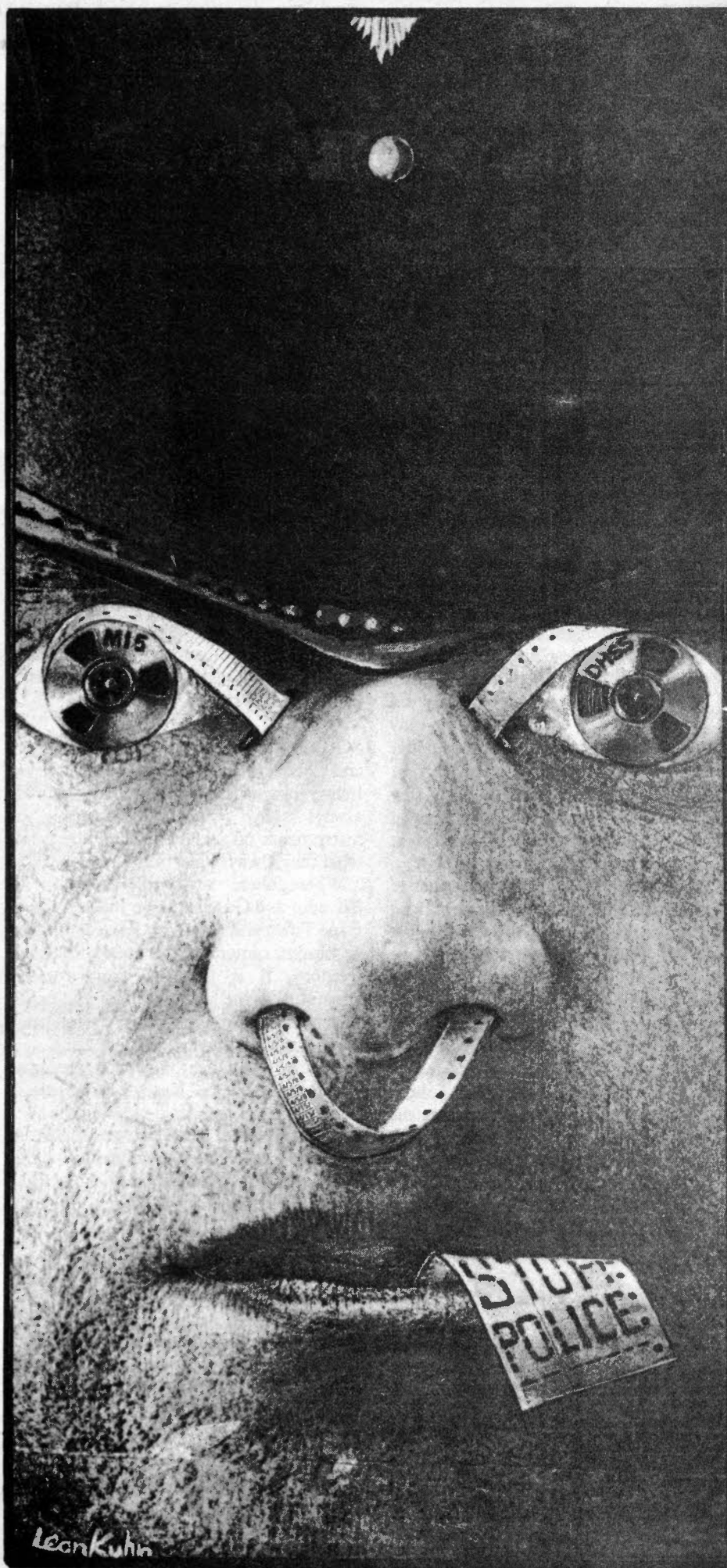
In these national, official job specifications, community police are instructed that they should aim at recruiting 'at least one informant in every street'. The community constable is instructed to cultivate the confidence of other officials whom the public trusts, and anyone 'who is in a position to give information' gained through personal confidence. The instructions say that the 'amount of information' passed to the Local Intelligence Officer by an area constable 'will indicate his effectiveness'.

The basis for a nationwide network of informants and memory databanks is thus already in place. About twenty per cent of the entire adult population are already on local police files. The files include not just those accused, convicted or suspected of crime — but also all the victims of crime, the witnesses and anyone else who 'comes to notice' of the police.

Cross referenced against each personal dossier may be addresses, vehicles used, often the names of children, parents, or relatives, the type of home they have and any piece of gossip, rumour, or observation that has ever been recorded.

A second facet of this national information system is the Police National Computer. This is the most active official computer databank now in operation in Britain. In the ten years since it was set up, the number of files stored has grown from a few hundred thousand to over 50 million.

Another facet of this technology is the linking of computers. One effect of linking the Police National Computer to many



other computers has already been to create a system of partial population registration — without asking parliament. Since 1974, through the vehicle and driving licence computer, more than half the adults in the country have had to keep the police computer notified of their current address.

The DHSS's new Departmental Central Index will be a comprehensive and efficient population register. It will contain almost everyone's age, address, financial status and family circumstances, taxes paid and benefits claimed. Its contents may be transferred, almost at whim, to police, tax, or security computers. Yet in making its plans for the Central Index, the government has not seen fit to debate the issues of principle involved. In the planning of this new scheme, I have yet to see a single reference to the issue of human rights or the dangers to liberty involved in creating a national population register. Nor has there been any reference to the need for greater public accountability of the officials involved, or a discussion of how to provide independent safeguards on how information may be used.

If we do ever get to a complete 'Big Brother' central databank, the first people I will blame will be the efficiency experts, who built the things just to make the system work better. They mean no ill, of course, but they owe no duty to making democracy work as well as their computers do.

IF YOU FIND THAT news of computer databanks discomfiting, I ask you to remember that the computers did not create these threats. The problem throughout has been the cavalier attitudes and actions of bureaucrats — and the subsequent public acquiescence in what they have done.

By focussing on technology alone, the problem of resisting authoritarianism as a political system inevitably appears as remote and inhuman, as something which the ordinary person can never hope to control. Such an approach puts beyond reach the problem of protecting privacy and freedom from the encroachment of technology.

Big Brother was and is a *political* vision. The threats which technology poses for liberty are also political in their origin and effect. To look at the danger of totalitarianism through its technology alone misses the point. It means we blunt or sacrifice our vital protective instincts on behalf of liberty.

For an illustration, take telephone tapping. People frequently express fears about tapping, whereas they do not seem to fear the possible presence of informers and snoopers in the guise of friends. I have never received a letter which suggests that a friend is an informer to the political police or the state security service.

Yet the most important way in which all secret police forces acquire personal data —

Leon Kuhn

other than from open sources — is from informants inside a group under surveillance. They may be planted agents or simply recruited. Understandably, it is easier to believe that if one is being watched, it is by the impersonal agent of a telephone tap, rather than by a friend or colleague. Yet it is they who are the main source of information about us.

THE MOST CRITICAL question about state surveillance is: what is done with the information gathered? Information on its own is of no consequence. It may as well not exist if it is not used.

The Police National Computer system provides a good example of the active use of information. It has a rapid communications network extending across the country, with video terminals in every major police station. From there, a radio system connects the computer to every police officer out on the streets. Information is normally made available within a few seconds of an enquiry being made.

This rapid access to information affects how the police deal with the public. Without the computer, police officers must make close and co-operative links with the whole community to obtain the information needed to clear up crime.

But with the computer networks, with the Local Intelligence databanks, society as a whole is put under surveillance, and the police objective alters. In order to be able to use the PNC most effectively, police officers must make as many checks as possible on each individual, in order to find the few that the computer singles out for special action. This process is called stop-checking. It requires no social support; indeed, it sacrifices any.

The random stopping of citizens to make a check on police computer records has no lawful basis. But it happens. This year, there will be over 10 million police computer checks on innocent people. According to the police and the government's own reports, between 90 and 99.5 per cent of all checks are on innocent people. This is not surprising — the idea is to check on what the computer has to say about as many people as possible.

On the basis of databank information — which may or may not be accurate, may or may not be legally acquired — those in authority can decide how to treat individuals. The police can, for instance, inflict extra-judicial punishments, such as harassing a citizen without the sanction of a court, or the process of publicly testing evidence. Inside security agencies, this practice is called 'countering'. It means actively disrupting the lives of those who do not accept the status quo, even though what they do and say is wholly within the law.

Last year it was shown that wholly inaccurate and extremely damaging information had for years secretly been

passed on by the security services to managers of the BBC, blighting the careers of prospective television and radio employees.

Vetting processes which depend on a supply of secret personal information are also prevalent in the civil service and in British industry. This information has been used systematically to deny employment opportunities to people whom those in power considered to hold 'subversive' opinions.

SUBVERSION IS A dangerous word. The evident view of many in authority is that to disagree with the status quo is inherently anti-social. Official instructions to police Special Branches order them to keep watch on anyone who, in their view, might at some future time do something which might have an effect on public order. These official instructions allow this peculiarly political police force to extend the watch on so-called subversives as widely as they wish, or have resources for. This has in the recent past included mothers organising demonstrations for better crèche facilities. They were systematically watched and photographed as they and their infants celebrated outside local authority offices.

The existence of camera technology did not create such a situation. Arrogantly unaccountable and undemocratic police practices, and a complacent executive, did.

It is that sharp end of surveillance that matters most. It was the same in the novel *1984*. It was not Big Brother's omnipresent telescreens that actually caused oppression, but the public knowledge of what happened when you said something out of line in front of them. Above all, it was the fear of what would follow behind the windowless facade of the Ministry of Love.

Totalitarian systems of political control are about influencing the behaviour of many by the calibre of treatment that a few receive. The boundaries of freedom are determined by the behaviour of the state towards those who approach or cross the boundaries the state tries to set.

From this, it follows that the safety mechanisms needed to combat oppressive technology are, of necessity, political. They should address not the technologies *per se*, but instead create countervailing legal and bureaucratic structures which protect liberty, and ensure a plural, democratic society.

The first safety mechanism we need is a system of checks and balances, of controls on executive activity. To start with, that means a parliament, judiciary, press, who are independent of — not subservient to and worshipful of — the executive. Today, these institutions are increasingly dominated by supplicants and patrons of the current regime.

The second safety mechanism is the robust defence of fundamental human

rights. Far too often, those who wish their privacy and liberty to be defended are asked: What have you got to hide? Such questioners cannot be serious. There is nothing unreasonable in insisting that individuals should have rights to control how personal information about them is handled. To argue otherwise is to suggest that the agencies and organisations who act in our name are always benignly motivated, act without prejudice of view, are even-handed in their objectives, staffed at every level with individuals who operate with impeccable care, total honesty and consistent diligence. What nonsense!

The third and most important safety mechanism is to strengthen the democratic accountability of the institutions permitted to hold a monopoly of the use of force. The problem here is to make these administrators accountable to the community — not the other way round.

The propriety of the law, and the legitimacy of the police force derive only from the common desires and aspirations of the civic community. When, as is happening increasingly, that community feels the 'chilling effect', it is not a sign of their growing unreason. It is a signal that the institutions of government are losing balance and becoming authoritarian.

SO DO NOT be distracted by computers and video screens. Recognise the enemies of liberty for who they really are, and who they always have been. Recognise the instruments of the enemies of liberty for what they always have been.

Where there is trouble now, in El Salvador and Guatemala, in Johannesburg, Cape Town and Soweto, it is not computers or monitor cameras that are taking lives and freedom. It is the old, familiar, ugly apparatus — the acrid-smelling end of the policeman's gun, the heavy riot stick lancing the air, the boot in the kidneys. It is the quieter violence of being forced into poverty and silence. It is the same here in Britain.

What we need are checks and balances: effectively enforceable fundamental rights; democratic accountability of the police and other institutions; freedom of information. Have these needs not already widely been recognised? So the problems of controlling oppressive technology are then not hopeless?

Yes, but — in Britain now, the trends of government action are all away from accountability, and democracy, and against human rights. New laws and practices have greatly extended coercive powers, and diminished accountability.

Technology can be controlled. It is under control already. But by the wrong people. □

The text of this week's Opinions programme appears by arrangement with Channel 4 and Panoptic.