

# Paranoid Androids?

## One Nation Under a Barcode

Great Britain, 1999: state snooping, intelligence gathering, and covert spy work is no longer just the job of shady police and security bodies like MI5, Special Branch, the Met and co. These days Orwellian state surveillance and Big Brother technology is an essential cog in the cold consumer machine. Behind the computer screens, telephones and spy camera lenses, the UK surveillance technology industry is worth £2 billion a year. Department of Social Security (DSS) fraud investigators, rail ticket collectors [aka Revenue Protection Officers!], TV license squads, and private security firms like Group 4 are employed to work as the 'Little Brothers' for the Big Brother law enforcement agencies. Surveillance is a part of the daily routine.

Employees are monitored for performance on the basis of conversations recorded or footage filmed during the day. Superstore loyalty cards are screened to identify individuals by their consumer habits, credit rating, and marketing potential. And inside the home—every phone call made, internet site visited, or even programme watched on pay-by-view digital television leaves a potential information trail to the door of the law enforcement agencies.

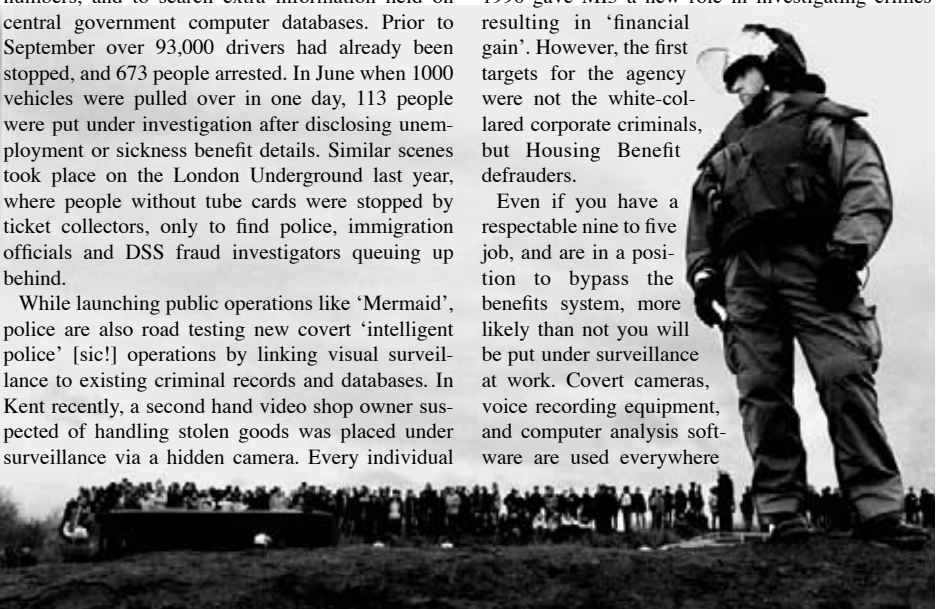
Stop and search powers are being used by police across the UK to target "illegal immigrants, benefits cheats and anyone 'of interest' to the police"<sup>1</sup>, under the Public Relations cover of a national clampdown on dangerous cars. In September 1998, as part of an ongoing campaign known as 'Operation Mermaid', police roadblocks were set up with immigration, DSS and Customs and Excise officials ready to interrogate passing drivers. Mobile data terminals were used to check license plates, National Insurance (NI) numbers, and to search extra information held on central government computer databases. Prior to September over 93,000 drivers had already been stopped, and 673 people arrested. In June when 1000 vehicles were pulled over in one day, 113 people were put under investigation after disclosing unemployment or sickness benefit details. Similar scenes took place on the London Underground last year, where people without tube cards were stopped by ticket collectors, only to find police, immigration officials and DSS fraud investigators queuing up behind.

While launching public operations like 'Mermaid', police are also road testing new covert 'intelligent police' [sic!] operations by linking visual surveillance to existing criminal records and databases. In Kent recently, a second hand video shop owner suspected of handling stolen goods was placed under surveillance via a hidden camera. Every individual

entering and leaving the shop was scanned against police databases to build up a chart of colleagues and friends. The police then passed on this information to the DSS, Trading Standards and Health and Safety, and the owner and colleagues ended up in court. The shop ended up closed; yet the owner had no idea of the covert surveillance that had taken place.

This operation, known as computer data matching, is turning individual government and police systems into a single giant electronic driftnet, in which any one department can interrogate data from any other. For example, under the Social Security Administration (Fraud) Act, the DSS were given the power to check data from systems run by the Inland Revenue and Customs and Excise<sup>2</sup>. DSS fraud investigators can also check information held on the Home Office immigration, emigration, passport and prisons databases. And as if all these investigative powers were not enough, the Security Service Act of 1996 gave MI5 a new role in investigating crimes resulting in 'financial gain'. However, the first targets for the agency were not the white-collared corporate criminals, but Housing Benefit defrauders.

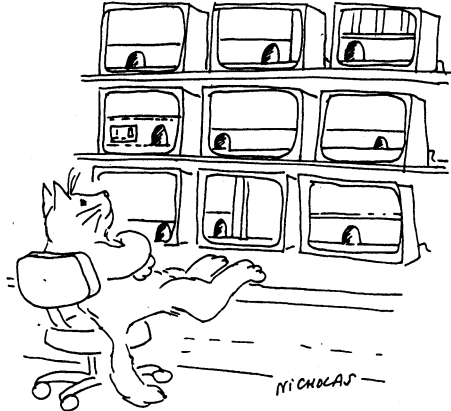
Even if you have a respectable nine to five job, and are in a position to bypass the benefits system, more likely than not you will be put under surveillance at work. Covert cameras, voice recording equipment, and computer analysis software are used everywhere



# PARANOIA ZOO ZOO ZOO

to track and monitor individuals in the workplace. Cashiers working in supermarkets are logged on to a mainframe computer and checked for the rate of baked bean cans they scan in a day. Phone operators employed in telephone call centres are eavesdropped on and their Call Handling Time performance moni-

time internet use and e-mail traffic. In December 1998 Statewatch revealed that the EU Council of Justice are pushing through legislation forcing all Internet Service Providers (ISPs) to hand over the account numbers and personal billing information of any individual subscriber on production of a warrant<sup>6</sup>. Like phone tapping, the authorities will be able to examine web surfing patterns and personal e-mails as they are sent over the net. Looking like a Euro-Police Act for the information age, the grounds for getting a warrant will "be infinitely extended to all forms of offence including public order or 'national security'"<sup>7</sup>.



Travelling over physical national borders in Fortress Europe is getting tighter too, whether going to a festival, a demo or a football fixture. Since the Heysel Stadium disaster in May 1985, football fans have been picked out for special state surveillance. They are logged on databases, recorded on CCTV, with exclusion orders, undercover football 'spotters', and hooligan 'hotlines' all being used to keep fans down and the multinational sponsors and broadcasters smiling<sup>8</sup>. The Metropolitan Police Forward Intelligence Team (FIT) was at least initially aimed at both football fans (e.g. at Euro 96) and political activists (primarily Reclaim the Streets). The fact that the two are linked in this way says something quite revealing about policing priorities and attitudes<sup>9</sup>. Every year the National Criminal Intelligence Service (NCIS) receives around 5,500 intelligence reports on football fans from the 92 English pro league clubs<sup>10</sup>. Inside the Football Unit of the NCIS this intelligence is catalogued, analysed and filed on to the database and made available to all UK police forces. Every time fans go abroad, these files are made available to their European police counterparts, and in the case of two Cardiff City fans, some are stopped, arrested, interrogated and then deported back to the UK<sup>11</sup>.

tored<sup>3</sup>. In most large chain stores CCTV is specifically used to watch the workers, as well as scanning for shoplifters. Theme pubs and petrol stations position CCTV cameras over the tills to monitor all cash transactions, and over computer terminals to watch over the operators.

Today, employers can investigate a person's lifestyle and history before hiring them. Under the 1997 Police Act staff managers can look at criminal conviction certificates held on police databases<sup>4</sup>. Random drug tests are appearing in the workplace, written in the fine print of the contract, or even made a compulsory part of the interview process. Recruitment agencies automatically screen employees through extensive references, computerised personality and psychology tests, and in some cases, handwriting analysis. A recent report into workplace privacy by the Institute of Employment Rights said that British employees were the most monitored in Europe<sup>5</sup>. In the same way that banks are using data profiles of customers to track credit rating and spending patterns, the UK workforce is being put under the surveillance microscope and filed for future reference.

On the 26th May 1997, the EU Council of Justice passed legislation allowing national police and security agencies to link up databases, conduct joint surveillance operations, and share information on anyone travelling in large groups to "political demonstrations, pop concerts, environmental protests and sports fixtures"<sup>12</sup>. Since then Trans-European police operations have begun to concentrate on the intelligence angle. For example, Danish bikers travelling to the 1998 Custom Bike Festival were identified by Kent police from digital mug shots held on the Schengen Information System (SIS). And official figures show the SIS currently holds over 3.5 million

Online, freedom in cyberspace is being challenged byte for byte by the new technology and backdoor legislation mobilised by law enforcement agencies to police the internet. All EU national police forces will soon have the power to monitor an individual's real



records on file, including information on asylum seekers, immigrants, drug users and campaigners<sup>13</sup>. In September last year, 50 people attending a People's Global Action seminar in Geneva were arrested in a dawn raid. Illegally detained, they were photographed, fingerprinted, and photocopies made of their passports. No information was available to say whether this material would be destroyed, stored on Swiss databases, or made available to European police on the Schengen system.

### Don't Get Too Paranoid...

In the UK, government and corporations are linking technological arms, building surveillance mechanisms into every corner of society. It is impossible to estimate the scale of all this technology and of state intrusions into our lives. Personal anonymity is being erased with every new computer system and closed-circuit camera.

But it is worth remembering the restraints this technology operates under. They are restrained by the cost of the technology and they are restrained even more by the cost of labour. It costs £100 million a year in wages just to monitor CCTV systems in the UK. Ultimately the technology has to be maintained by humans, and is vulnerable to human error. Networks will fail, systems will crash and data will be 'unrecoverable'. Surveillance operations cost time, money, and manpower, and Big Brother stings like 'Operation Mermaid' are designed primarily to intimidate the population into compliance.

Therefore we shouldn't be frightened by these 'crackdowns', precisely because that is their primary purpose. They rely on fear and paranoia to achieve a deterrent effect—they will swoop in, make examples of a few people and then be gone again. DSS roadblocks, benefit fraud crackdowns, yellow hat inspectors on the trains, drugs squads complete with sniffer dogs that make periodic raids on train stations—all of these are too expensive to be used all the time—they are confined to particular areas and to a short space of time. With a little bit of intelligence it is still possible to play on their weaknesses and stay one step ahead of the state surveillance machine...

### Fight Back!

- Consider every piece of data as a weapon that may potentially be used against you—from an address on a competition form to the information contained on the electoral register (voting information has been passed on to the Inland Revenue and the DSS in the past). When putting your real name to

anything use only one initial as two will give a more accurate match on computer files.

- Multiple identities are not difficult to manufacture. Reverse initials on forms and bills, change two digits of your NI number, and give as little information as necessary.
- Think about the phone calls you are making. BT will sometimes pass on billing information direct to police, who use analysis software to create personal profiles of contact networks, friends etc. When planning actions don't run through the entire phone tree in one go—or you could inadvertently end up disclosing more information than necessary.
- Employers have to inform you if they intend to record your calls, film you at work or monitor your e-mails. A number of cases have upheld this point in the European Court of Human Rights under Article 8 of the UN Declaration of Human Rights. With e-mail, unless you are using strong encryption, assume that every mail you send is an open letter that can be read by anyone. Use encryption software like Pretty Good Privacy which is available as freeware on the internet at: <http://www.pgpinternational.com> Alternatively, use free e-mail services to set up a temporary line of communication when organising actions, registering in a false name (see box on the J18 website in *June 18th* article on page 31).
- Apply to local councils, businesses and police to see camera footage taken of you. Under the European Data Protection Directive you have a right to see what data and images are held on you. Applications for information are made through the UK Data Protection Registrar.
- Likewise, apply to see what information is held on government files. You can apply to civil agencies like the DSS, or police authorities like the NCIS to see what information is held on file. For more information contact the UK Data Protection Registrar.
- Silence, non-disclosure and duplicity is the best route to retaining anonymity and creating multiple identities. One individual in the US who ended up in court for holding false documents got a medical note to say that he had temporary amnesia and couldn't remember filling out the original forms. He was found not guilty. Use your imagination and let that split personality run wild!

(For more suggestions on becoming 'invisible' see 'Now You See Me...' section in *From Knapping To Crapping* on page 302.)

# PARANOIA 20-20-20

## Contacts

**Privacy International**, PO Box 3157, Brighton, BN2 2SS, East Sussex, UK.  
Website: <http://www.privacy.org>

**Statewatch**, PO Box 1516, London, N16 0EW, UK.  
Website: <http://www.statewatch.org>

**UK Data Protection Registrar**, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, UK.

Website: <http://www.hms.gov.uk/acts/acts1998/19980029.htm>

**Privacy Internationals** 'Big Brother Survival Kit' is recommended. Contact *Privacy International* or for information e-mail: [bbsurvivalkit@yahoo.com](mailto:bbsurvivalkit@yahoo.com)

## Footnotes

- 1 Privacy International website: [www.privacy.org](http://www.privacy.org)
- 2 Computer Weekly, 05/12/96.
- 3 Communication Workers Union, 150 The Broadway, London, SW19 1RX.
- 4 Section 5, 100-110, Police Act 1997.
- 5 *Workplace Privacy*, IER, 177 Abbeville Road, London, SW4 9RL.
- 6 Statewatch, Vol. 8 No. 6.
- 7 Ibid.
- 8 *Surveillance, CCTV and Social Control*, Ashgate, 1998.
- 9 See 'The Empire Strikes Back', *Do or Die* No. 6, page 137.
- 10 NCIS Annual Report 1997, PO Box 8000, London, SE11 5EN, UK.
- 11 Case of the Boore Brothers. Contact Liberty, London, 1993.
- 12 Statewatch Report, 24/09/98.
- 13 *Under Surveillance* 1998 Justice, London, UK.

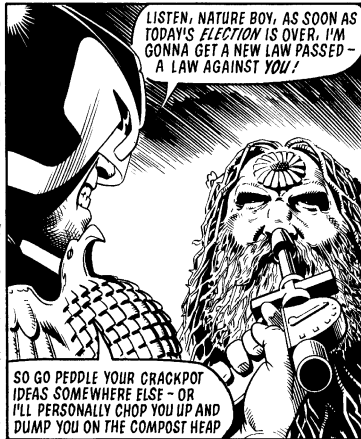
## Beware the fashion police...

*Waiter waiter, there's a cop in my suit!*

As reported in the *Earth First! Action Update* (No. 55, Jan/Feb '99, see p. 333 for contact details) a new law regarding covering your face to prevent identification—masking up—came into force on March 1st 1999. The Crime and Disorder Act 1998, Section 25-27, states that it "aim[s] at preventing violence by giving the police new powers to unmask potential violent offenders." This law can only be used if a police officer of Inspector rank or above fears "serious violence or disorder in his/her area" and gives an order for you to 'de-mask'. If you do not "remove any item which the constable reasonably believes you are wearing wholly or partly for the purpose of concealing your identity" then you can be arrested. They also have the power to confiscate and destroy the materials used to mask up with. The police have been swift in implementing this new law. According

to *SchNEWS* 209, 23rd April 1999, see page 333 for contact details) hunt saboteurs in Dorset were de-masked and their hooded tops confiscated after the police declared the whole county "an area of potential serious disorder". In Oxfordshire, Thames Valley Police used the new law at the anti-vivisection demonstrations at Hillgrove Farm, where they forced people to de-mask, arresting one person who refused to do so. It was also used in The City of London on June 18th (see page 1) where some people leaving Liverpool Street station had their masks pulled off by the police.

Rather than being intimidated into not masking up we must find ways around this law. One way to do



this is to encourage more people to wear masks on actions. The police may be able to demand the removal of 5 or 6 people's masks but 500 or 600 should be more of a problem. It should also provoke a more strategic, wider look at our tactics. Learning, and using, methods of dealing with surveillance teams, snatch squads and police intimidation of individuals must become second nature for us. Additionally the police can only de-mask us if they are there; so maybe we should be thinking about less 'set-piece' demonstrations and confrontations

with the police, and more about surprise hits and mobile actions on our own terms. Above all though, we mustn't be put off—whatever laws they throw at us, we'll be there, continuing to resist...

## Millennial Paranoia

*They're Coming to Take Us Away, HaHaHeeHee...*

From panic stories in the press, to drunken conversations in the pub and conspiracy theories in New Age mags—everyone's got something to say about the Millennium bug. Here's our penny's worth: if somebody tells you they know authoritatively what will happen as a result of the Millennium bug...don't believe them! Whether it's top programmers or speed freaks, the truth is that nobody knows. I'm placing my bets on hangovers and a bit of an anti-climax, the state however is not. Operating on either exclusive information or the precautionary principle the state is preparing for possible major chaos. This is not a deranged conspiracy theory—it comes directly from

# PARANOID ZOO

their mouths. A computer whizz commissioned to write a report for the Metropolitan Police said that he fears “panic and civil disorder as electricity, gas and water supplies fail. Hunger as food supplies dwindle. Gridlock in major cities as traffic lights go out.” (*The Guardian*, 26/5/99).

This Armageddon scenario is unlikely—but possible. More likely is major disruption for some local authorities. Interruption of benefit payments for a few weeks is possible in at least some areas, which could result in serious rioting. Whether any of this is going to happen nobody really knows, but as long ago as January the Association of Chief Police Officers revealed that “30 police forces [have] cancelled leave in anticipation of the collapse of public utilities” (*The Guardian*, 18/1/99). The National Crime Squad (the national police coordination organisation) has also cancelled all leave.

We will get our first inkling of what they intend with the policing of the eclipse (on August 11th ‘99) which they have admitted will in part be used as a Millennium training event. This is not surprising considering that the head of the police ‘Millennium Co-ordination Committee’ is John Evans—the Chief Constable of Devon and Cornwall. More worrying than the police preparations for the bug is the involvement of the military. In the same January article quoted above, Chief Constable Evans confirmed that “talks with [the] military are already underway in case of civil disruption as a result of the bug...Army helicopters are being made available to airlift the police to different parts of the country in the event of disturbances”. On July 18th *The Times* carried a front page article entitled ‘Soldiers pull out of Kosovo to deal with millennium bug chaos’. Though it’s worth taking the article with a pinch of salt it does make interesting reading—coming as it does from a newspaper close to the security services and read and written by the establishment.

“The SAS and other special services are to deal with outbreaks of civil disorder and the collapse of utilities under secret plans being drawn up by the armed forces to cope with the millennium bug...The extent of the military’s role has been disclosed as the armed services pre-

pare for the critical day of September 9, or 9/9/99, when the scale of the computer chaos could become apparent. Half the combat troops are to be withdrawn from Kosovo by the end of August, a total of up to 2,000 soldiers. [Operation Surety]...is designed to ensure that essential government and civilian [interesting distinction!] functions can continue between September and February...Planners fear that computer failures could leave installations vulnerable to criminal or terrorist attack. Armed troops, some with light tanks and heavy weapons, will be deployed to guard likely targets such as airports. In the worst scenario, some form of martial law might be necessary in localized areas. Eight leading financial institutions have asked the MoD for protection. Individual chief constables will call for military back-up if security system failures lead to looting and civil disorder... The Royal Navy will concentrate on the English Channel...The Royal Marines’ counter-terrorist unit and the Special Boat Squadron will be on stand-by to board ships...A decision on whether leave for the armed services should be cancelled over the millennium will be taken after September, when the extent of the problem could emerge. The military has been testing its new communications systems over the past two weeks. Problems have been discovered and senior officers say they may have to rely on older radio technology.”

Cynical as I am, when *The Times* talks about martial law, I start to worry. If you think ‘troops on the street is not the kind of thing that happens in this country’, look at Northern Ireland which has been under martial law for nearly thirty years [or think of the tanks outside major airports during the Gulf War]. My advice is not to get paranoid, but watch the unfolding situation. Read the papers aimed at the upper middle classes—see what they’re being told. If you’ve got friends or relatives in the forces ask them what—if anything—they’ve been told. Don’t scaremonger, and remain sceptical of anyone who tells you they know what’s going to happen. As I said earlier, I’m expecting a vast anti-climax. However it’s worth being well informed. As countless kids around campfires are taught to say—‘Be Prepared’.



THE REPRESSION LABORATORY



## Lessons from the North of Ireland—Anti-Terrorist Legislation

"...if we lose in Belfast we may have to fight in Brixton or Birmingham... Perhaps what is happening in Northern Ireland is a rehearsal for urban guerilla war..." - John Briggs MP, 1973.<sup>1</sup>

On 21st November 1974 bombs exploded in two Birmingham pubs, killing 21 people and injuring over 160. Within 8 days the *Prevention of Terrorism (Temporary Provisions) Act* was introduced. It took just 17 hours to pass and nobody voted against it. The Act included provisions for banning organisations, arbitrary arrest, powers to exclude people from Britain and detain suspects for seven days without charge, court hearing or appeal. People became guilty until proven innocent, and were often not even told what the charges against them were.<sup>2</sup>

Twenty-seven years of struggle in Northern Ireland have shown how the British State responds to political conflict and civil war. The role of law in Northern Ireland is characterised by the criminalisation of political dissidents, the militarisation of the police and the politicisation of the courts. Brigadier Frank Kitson, an influential figure in British law enforcement, wrote "The law should be used as just another weapon in the government's arsenal, and in this case it becomes little more than a propaganda cover for the disposal of unwanted members of the public".<sup>3</sup>

Policing in Northern Ireland is a "laboratory situation" for the problems facing British policing. The array of military-type hardware and the increasingly violent and militaristic trends in mainland Britain all had their test run in the policing of Ireland.<sup>4</sup> Now the government is attempting to impose permanent and sweeping anti-terrorist legislation that will take in everyone from the IRA through to Earth First!

In December 1998 the government published a consultation paper on *Legislation Against Terrorism*.<sup>5</sup> In the light of moves towards peace in Northern Ireland they propose to get rid of the temporary *Prevention of Terrorism (PTA)* and *Emergency Provisions (EPA)* Acts, replacing them with a permanent law, retaining many of the PTA's terrifying powers of arrest and detention<sup>6</sup> and extending them to domestic 'terrorism'—us!

The document states that "Animal rights, and to a lesser extent environmental rights activists, have mounted and continue to pursue, persistent and destructive campaigns... While the level of terrorist activity by such groups is lower, and the sophistication of their organisation and methods less well developed than that of some of the terrorist groups in Northern Ireland... there is nothing to indicate that the threat they pose will go away."<sup>7</sup>

Terrorism is to be defined as "the use of serious violence against persons or property, or the threat to use such violence, to intimidate or coerce a government, the public or any section of the public for political, religious or ideological ends." The term serious violence is used to include serious disruption, for example attacks on computer installations or public utilities.<sup>8</sup> Alarmingly, powers under Section 60 of the CJA, frequently used on demonstrations to allow random stop and searches, are triggered by "serious violence", *exactly* the same words as proposed for the new Act.<sup>9</sup>

Under the proposed legislation the government's powers to ban any organisation (or 'front' organisation) deemed terrorist would be extended to include domestic terrorists.<sup>10</sup> It is also proposed to make it an offence to collect, record or possess information which might be useful to terrorists<sup>11</sup>—this could mean the end of the Corporate Watch Address Book, Squaring Up to the Square Mile, or even lists of Genetic test sites!

Much of what results from these proposals depends on public opinion and media image. It is already easy for the government to begin to classify animal rights campaigners as terrorists, and recent coverage of ecological direct action—particularly the June 18th Carnival<sup>12</sup>—suggest that if they tried to classify us as terrorists the media would be unlikely to dissent. Consultation on the paper finished in March 1999, and the Home Office are considering the results. They would not comment on when it might become law...

1. *Political Trials in Britain* by Peter Hain (Pelican, 1985) p.235.
2. *Ibid.* p.228/230
3. *Low Intensity Operations: Subversion, Insurgency and Counter Insurgency* by Brigadier Frank Kitson (Faber, 1971) p.69
4. *Op. Cit.* Peter Hain, p.226/228
5. *Legislation Against Terrorism*, a consultation document published by the UK Government. It's also on the web at: [www.official-documents.co.uk/document/cm41/4178.html](http://www.official-documents.co.uk/document/cm41/4178.html)
6. *Ibid.* Particular Chapters 7 (Arrests) and 8 (Detention).
7. *Ibid.* Chapter 3 (Definition of Terrorism) para. 3.10 and 3.11
8. *Ibid.* Chapter 3, para 3.16 and 3.17
9. *Criminal Justice and Public Order Act*, 1994, Section 60.
10. *Legislation Against Terrorism*, Chapter 4 (Proscription).
11. *Legislation Against Terrorism*, Chapter 12 (Ancillary Offences).
12. *cf* Almost any of the UK national newspapers for Saturday June 19th 1999.