Privy Counsellor Review Committee

Anti-terrorism, Crime and Security Act 2001 Review: Report

Presented to Parliament pursuant to Section 122(5) of the Anti-terrorism, Crime and Security Act 2001

Ordered by The House of Commons *to be printed 18th December 2003*

HC 100 London: The Stationery Office £*zz*.00

12th December 2003

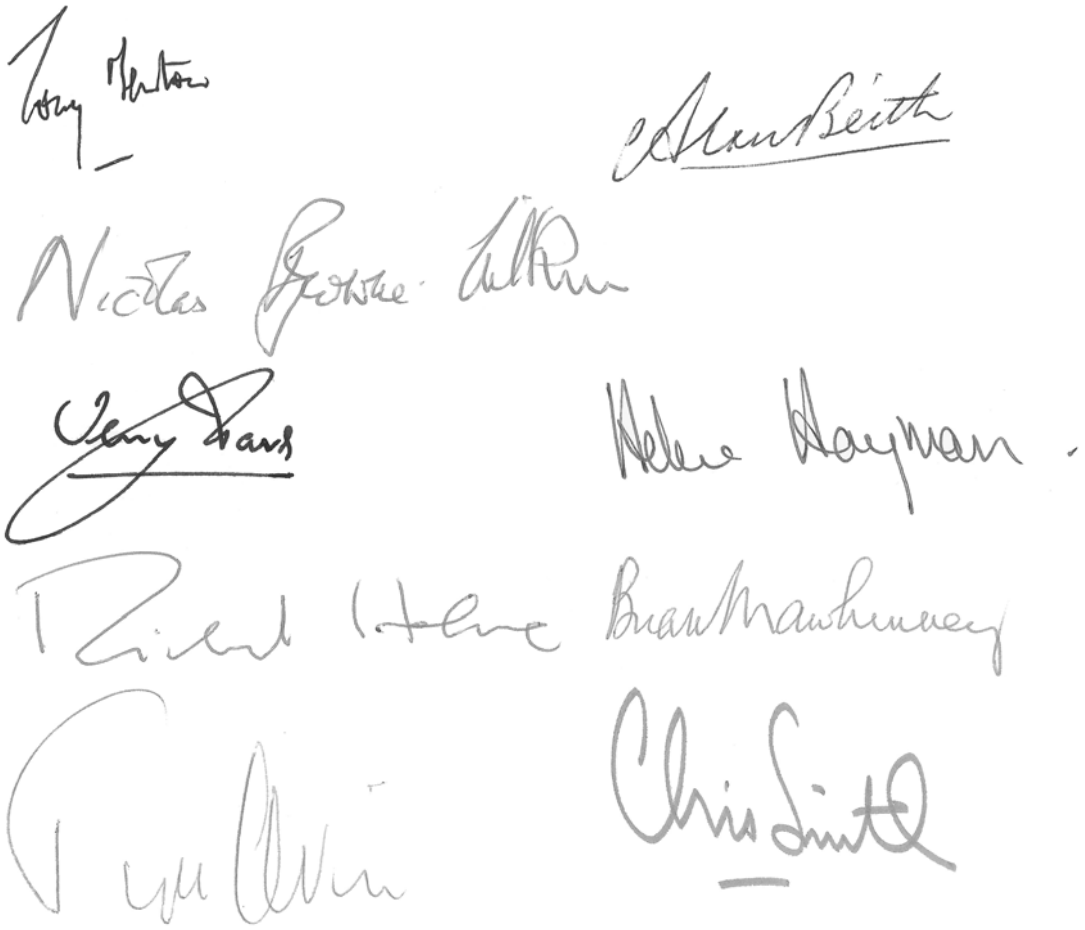
Anti-terrorism, Crime and Security Act 2001 Review

The Rt Hon David Blunkett, MP
Secretary of State for the Home Department

Dear Home Secretary,

In April 2002 you charged us with reviewing the Anti-terrorism, Crime and Security Act 2001 enacted following the attacks in the United States on 11th September 2001. We now enclose our report, in accordance with Section 122(4) of the Act, for laying before Parliament.

In doing so we would like to express our warm thanks to our small secretariat who have worked tirelessly to support the Committee: Angela Harris, John Pavel, Shabana Hariff and Alan Pitt. We would also like to express our gratitude to officials in the Home Office and to the wide range of other people and organisations who have contributed to our work.



The Rt Hon Lord Newton of Braintree (Chairman) ◦ The Rt Hon Alan Beith, MP (Deputy Chairman)
The Rt Hon The Lord Browne-Wilkinson ◦ The Rt Hon Terry Davis, MP ◦ The Rt Hon Baroness Hayman
The Rt Hon Lord Holme of Cheltenham ◦ The Rt Hon Sir Brian Mawhinney, MP ◦The Rt Hon Joyce Quin, MP
The Rt Hon Dr Chris Smith, MP

A.1: Contents

A.2: Foreword

The events of 11 September 2001 highlighted the existence of a formidable international terrorist threat, raising the prospect of further attacks on civilians on a previously inconceivable scale.

In response to this threat, the Government presented the Anti-terrorism, Crime and Security Bill 2001 to Parliament on 12th November 2001. It received Royal Assent on 14th December 2001.

The Act was wide in scope, including additional powers for the police, and measures relating to information sharing, and to the security of airports and laboratories. Amongst the most controversial measures were those contained in Part 4 which permit the potentially indefinite detention without charge of foreign nationals suspected of involvement with al Qaeda, and associated terrorist networks, but who cannot be prosecuted or deported; and those in Part 3 which allow public bodies to disclose information that has been obtained in pursuit of their own functions to assist criminal investigations and proceedings, here and abroad. The tax collection departments can also disclose information to the intelligence services.

The enactment of Part 4 required a derogation from the right to liberty under the European Convention on Human Rights. Other countries also introduced wide-ranging legislation as part of their response to the threat highlighted by the attacks on the USA. No other Council of Europe country has, however, found it necessary to seek a derogation from the Convention to give it powers to meet that threat.

In common with previous emergency legislation, the Act provided for independent review. We were appointed by the Home Secretary to the Review Committee in April 2002, charged with reporting to Parliament on the Act by December 2003.

Our starting point is that the ordinary criminal justice system and established security methods must remain the preferred approach to tackling the crime of terrorism.

Nevertheless, we recognise that special counter-terrorism legislation can be justified because of the way terrorists operate, which makes them hard to catch and convict, because of the risks that they pose to society, and because it is important to be able to pre-empt, as well as to deter, terrorism.

Such counter-terrorist legislation must be sufficiently flexible to meet the potential threat to society, but it must also contain proper protections for the privacy and liberty of the individual and, in our view, stand apart from other law so that it can be accompanied by its own tailored safeguards, including careful monitoring and review of its use. It is important that it commands broad public support, otherwise its use risks being mistrusted and therefore less effective.

In September 2002, the Home Secretary the Rt Hon David Blunkett MP commented: "Since the September 11th attacks, we have had some success in damaging al Qaeda's capability, and in thwarting attacks. But the terrorist threat remains real, and serious. As recent events have shown, no country is immune from attack, and it simply is not possible to guarantee against more attacks in the future." His statement remains valid

today. It is clear that the nature of the terrorist threat confronting the United Kingdom makes it prudent to assume that a special legislative response is likely to be required for the foreseeable future.

So far as the substance of the Act is concerned, we do not believe that Part 4 is a sustainable way of addressing the problem of terrorist suspects in the United Kingdom. The operation of these provisions has been subject to specific review and renewal since 2001: Lord Carlile of Berriew reports periodically on the operation of this Part, and appeals against certification by some of those detained under it have been heard before the Special Immigration Appeals Commission. We are satisfied in the light of these other assessments that the measures – as they stand – have not been used injudiciously or excessively, but Part 4 raises difficult issues of principle and we do not believe that it meets the full extent of the terrorist threat. It applies only to foreign nationals and although the legislation is expressed in terms of international terrorism, the scope of the derogation from the European Convention on Human Rights means that it can only be applied to individuals with links to groups linked to Al Qaeda. It should be replaced.

We have also considered the way in which this wide-ranging Bill was examined before enactment. By definition, an emergency timetable does not allow the normal opportunities for full and detailed Parliamentary scrutiny. Enacting provisions in this way that apply to all crime, and not just to terrorism, including provisions which had previously been rejected by Parliament, ran the risk of undermining the usual consensus for recognising the responsibility of the Government of the day for public safety and for giving it greater discretion when approving legislation presented under emergency conditions. This underlines the importance of restricting emergency legislation of this sort to dealing with terrorism, rather than using it as a vehicle for addressing more general criminal justice issues.

In conducting our review we have taken evidence from a variety of sources. Legislation of this sort is of most direct practical concern to the counter-terrorist authorities which use it. Thus we have taken evidence from the police, the security and intelligence agencies and other counter-terrorist officials. We have also looked beyond the authorities, consulting academics, lawyers and other independent commentators and experts. In addition we have made a number of field visits: to the Special Immigration Appeals Commission appeals hearings, to prisons holding detainees under the Act, and to airport police amongst others.

Terrorist networks have attained a global reach, and the threat which they pose requires an internationally co-ordinated approach; not only in parallel legislation where possible, but in the regular exchange of information and best practice and in enhanced practical co-operation across borders. We have, therefore, also taken account of the experience of other countries since 2001, particularly that of the United States, and we have taken evidence from a French counter-terrorist judge.

New legal powers are only a part of the total counter-terrorism effort. We have not attempted to assess the Government's wider counter-terrorist strategy; however, where we have found gaps, we have drawn attention to them.

The material which follows the summary of our conclusions and background to the Act discusses individual rights and public safety. We outline the principles according to which we think counter-terrorism legislation ought to be framed and describe our methodology. The detailed report which follows is structured according to the order of the Act.

B: Conclusions

B.1: Principal conclusions

Principles

Our conclusions flow from the application of two main principles:

- that the individual has a right to liberty and to privacy; and
- that the authorities have a duty to take the steps necessary to protect society from terrorism.

Conclusions

1. **Terrorists are criminals, and therefore ordinary criminal justice and security provisions** should, so far as possible, continue to be the preferred way of countering terrorism.

2. **There is, however, a continuing need for special counter-terrorism legislation**. This counter-terrorism legislation should be:

   a. kept distinct from mainstream criminal law;

   b. limited to dealing with terrorism;

   c. accompanied by tailored safeguards;

   d. consistent with collective counter-terrorism policies agreed and coordinated by the international community.

3. **Special counter-terrorism legislation should be kept separate from general crime and security legislation**. The enactment of mainstream legislation using emergency procedures undermines the consensus for the use of such procedures in justifiable cases. The Anti-terrorism, Crime and Security Act 2001 provisions which are not specifically targeted at terrorism should be reconsidered, on their own merits, in the context of the mainstream legislation in which they belong. For example:

   a. the powers which allow public bodies such as the Inland Revenue to disclose information to help investigations and prosecutions, here and abroad, are not limited to terrorism cases. Disclosure of information held by public bodies should be subject to **additional oversight and safeguards proportionate to the seriousness of the crime and the sensitivity of the information sought**;

   b. the open-ended powers to require phone and internet companies to retain billing information and call data for national security-related purposes should be replaced by **mainstream powers which require communications data to be retained beyond its usefulness to the company for up to one year** and should be accompanied by strictly enforced access rules designed to protect privacy.

4. **We strongly recommend that the powers which allow foreign nationals to be detained potentially indefinitely should be replaced as a matter of urgency.** New legislation should:

a. deal with all terrorism, whatever its origin or the nationality of its suspected perpetrators; and

b. not require a derogation from the European Convention on Human Rights.

5. **We have identified several alternative approaches that, either alone or in combination, merit further development by the Government.**

6. **For example, the blanket ban on the use of intercepted communications as evidence in court should be lifted** to make it possible to prosecute more terrorists (and other serious criminals) and **the Government should examine the scope for more intensive use of surveillance to prevent and disrupt terrorism.**

7. **We broadly support the objective of strengthening some specifically counter-terrorist powers related to the financing of terrorism, the freezing of the assets of foreign individuals, the fingerprinting of terrorist suspects and targeting those who withhold information about terrorist offences, but there is a need for better safeguards in some cases.**

8. **The security arrangements relating to weapons of mass destruction, noxious substances, pathogens and toxins, the nuclear industry and aviation are welcome, but need to be enhanced**.

9. **We welcome the Government's increased determination to combat identity theft, but believe the relevant provisions of the Act do not address this problem adequately.**

10. **The powers which enable the Government to amend any provision of the Act without primary legislation should be repealed.**

Section 123 provisions

11. Section 123 of the Act gives our Committee the power to specify any provision of the Act which will cease to have effect 6 months after this Report is laid unless "a motion has been made in each House of Parliament considering the Report".

12. This provision was introduced in response to requests for the Act to be made subject to periodic Parliamentary review and renewal.[1] We agree that, as a matter of principle, emergency legislation ought to be subject to such scrutiny. While some provisions of the Act are already subject to periodic review and renewal,[2] **we recommend that Parliamentary debates, separate from the renewal debates, be held on this Report as a whole.**

13. **We therefore specify the whole Act, for the purposes of Section 123**. We recognise that this means that the Act would cease to have effect unless Parliamentary time was made available to debate the content of the Report, but we are sure that the Government will ensure that such a debate takes place. So our specification should not be taken as a recommendation to repeal the whole Act – there are a number of Parts of the Act which we welcome – but as a way of making clear our support for the principle of making emergency legislation subject to periodic review and renewal by Parliament.

[1] See the debates in the House of Lords and House of Commons on 10th, 12th and 13th December 2001 annexed at page 106ff.
[2] Anti-terrorism, Crime and Security Act, Sections 29 and 105.

B.2: Consolidated conclusions

General

14. **The idea of a durable body of properly considered, principled, counter-terrorist legislation — which is distinct from mainstream criminal law, addresses this particular threat to society and includes adequate safeguards of the rights of the individual — remains compelling. This was the Government's stated objective when it introduced the Terrorism Act 2000, and it is the approach to which in our view the Government should return. [Paragraph 111ff]**

Part 1 (Terrorist Property)

15. **Schedule 1 extends the power of the police to seize 'terrorist cash' at the borders (and pursue its eventual forfeiture through civil proceedings) throughout the United Kingdom generally. Three amendments would enhance its effectiveness and fairness.**

    a. **Open hearings in an ordinary Magistrates' Court are not the appropriate forum for handling cash seizures in terrorist cases. Such hearings are relatively infrequent and often depend on sensitive intelligence that the police may not be able to convert into open evidence within the 48 hours currently permitted between the seizure and confirmation in court. The procedure for warrant hearings in arrests under the Terrorism Act makes special provision for these difficulties. In our view, the Terrorism Act should be further amended to enable initial cash seizure hearings to be handled similarly, subject to later confirmation in open court under the normal rules of evidence.**

    b. **Powers of seizure should be extended to non-cash items where the police can show that they will have a direct role in preparing for, or carrying out, acts of terrorism.**

    c. **The provision that cash is to be held in an interest-bearing account during the course of proceedings is designed to compensate the individual where a terrorist link proves unfounded. Alternative means of compensation in cash seizure cases for those Muslims with religious objections to profiting from interest should be devised. [Paragraph 124]**

16. **The Government should report to Parliament during the debates on this Committee's Report on whether it is likely that there will be any further use of the Schedule 2 account monitoring orders – and, if it is proposed to retain the power, on the action that they propose to take to give them a realistic practical foundation. We draw this matter to the attention of the Treasury and Home Affairs Select Committees. [Paragraph 127ff]**

17. **Some mechanism for sharing more specific information on terrorist finance and reporting requirements should be developed between the law enforcement authorities and the financial services industry. We draw this to the attention of the Treasury and Home Affairs Select Committees. [Paragraph 132ff]**

18. **The legislation requiring the regulated sector of the financial industry to submit reports regarding their clients' activities should be amended to protect the privacy of innocent individuals and bodies corporate, by requiring the authorities to destroy reports in cases where charges are not brought or are disproved. An exception should be made only where appropriate authorisation is given that the report in question is material to an ongoing terrorist investigation. [Paragraph 134ff]**

Part 2 (Freezing Orders)

19. **Freezing orders for specific use against terrorism should be addressed again in primary terrorism legislation, based on the well-tested provisions of the Terrorism (United Nations Measures) Order 2001.**

20. **Freezing orders for other emergency circumstances, and the safeguards which should accompany them, should be reconsidered on their own merits in the context of more appropriate legislation for emergencies; the present Part 2 powers should then lapse. The forthcoming Civil Contingencies Bill would seem to be a suitable opportunity. [Paragraph 146ff]**

Part 3 (Disclosure of Information)

21. **The Government should legislate to provide independent external oversight of the whole disclosure regime (e.g. by the Information or one of the other statutory Commissioners) to provide a safeguard against abuse and to ensure that rigorous procedural standards governing disclosure are applied across the range of public bodies, prosecuting authorities and intelligence and security agencies. It should also require the independent overseer to publish statistics twice a year on the use of Part 3 (both within the United Kingdom, and to overseas authorities). [Paragraph 160ff; see also paragraph 53]**

22. **In our view, internal authorisation by a senior person would be adequate for the disclosure of addresses or phone numbers in terrorism cases.**

23. **While we accept that it may well be that the same regime could be justified for other types of serious crime, we would argue that prior judicial approval should be required in any case involving less serious crimes or the disclosure of more sensitive information. Parliament should be given the opportunity to decide what level of authorisation should be required, depending on the seriousness of the crime and the sensitivity of the information being disclosed. [Paragraph 167ff]**

Part 4 (Immigration and Asylum)

24. **We strongly support the Government's stated objective of prosecuting terrorists using the normal criminal justice system as the preferred approach. [Paragraph 205]**

25. **We strongly recommend that the powers which allow foreign nationals to be detained potentially indefinitely should be replaced as a matter of urgency. New legislation should:**

    a. **deal with all terrorism, whatever its origin or the nationality of its suspected perpetrators; and**

b. **not require a derogation from the European Convention on Human Rights. [Paragraph 185ff]**

26. **We set out below several alternative approaches that, in our view, whether alone or in combination, merit further development by the Government as possible bases for a more acceptable and sustainable approach, while the threat remains. There may be others. [Paragraph 204 ff]**

a. **It might be feasible to:**

i. **define a set of offences which are characteristic of terrorism and for which it should be possible to prosecute without relying on sensitive material, but**

ii. **raise the potential penalty where there are links with terrorism. [Paragraph 216ff]**

b. **One way of making it possible to prosecute in more cases would be to remove the UK's self-imposed blanket ban on the use of intercepted communications in court. [Paragraph 208 ff]**

c. **Another approach to the problem of confronting the suspect with specific accusations and evidence, without damaging intelligence sources and techniques, would be to make a security-cleared judge responsible for assembling a fair, answerable case, based on a full range of both sensitive and non-sensitive material. This would then be tried in a conventional way by a different judge. Despite the obvious difficulties, it would be worth working up more detailed proposals for an investigative approach for the specialised purpose of handling terrorism cases, where conventional prosecution might risk disclosing sensitive sources, or the available intelligence might not be admissible as evidence. [Paragraph 224ff]**

d. **Although the present public interest immunity rules already permit a certain amount of editing and summarisation there would be merit in developing a more structured disclosure process that is better designed to allow the reconciliation of the needs of national security with the rights of the accused to a fair trial. [Paragraph 236ff]**

e. **Under current arrangements in England and Wales the court is not party to plea bargains (although it is made aware of them and can volunteer disapproval) and any reduction in sentence in return for co-operation is at the discretion of the judge. There may, however, be particular merit in terrorism cases in giving the suspect greater certainty of outcome in the event of co-operation by establishing a sentencing framework within which the accused may be sure of securing a reduced sentence in return for co-operation. [Paragraph 240ff]**

27. **The Government should examine the scope for more intensive use of surveillance and we draw this view to the attention of the Intelligence and Security Committee, so that they can take account of it in their scrutiny of the intelligence and security agencies. We have in mind not simply the marking of particular individuals, but also training, the use of technology and better liaison between different agencies at ports of entry. [Paragraph 244ff]**

28. **It is possible that, even adopting some or all of the measures above, it may not be possible to prosecute in every case. The alternatives listed below would allow steps to be taken against both UK and foreign terrorist suspects which are less damaging**

to human rights than the current process (and so remove the need for derogation from the ECHR). These measures are much less attractive than conventional prosecution but in our view they are preferable to Part 4 as it stands. [Paragraph 250]

a. **The current Special Immigration Appeals Commission regime is used in cases which involve the detention of foreign nationals without charge. It would be less damaging to an individual's civil liberties to *impose restrictions* on:**

   i. **the suspect's freedom of movement (e.g., curfews, tagging, daily reporting to a police station); and**

   ii. **the suspect's ability to use financial services, communicate or associate freely (e.g., requiring them to use only certain specified phones or bank or internet accounts, which might be monitored);**

   subject to the proviso that if the terms of the order were broken, custodial detention would follow. [Paragraph 251ff]

b. **In cases where deportation is considered the only possible approach — and we have considerable reservations about it as a way of dealing with suspected international terrorists — we have seen no evidence that it would be illegal for the Government to detain the deportee while taking active steps in good faith to reach an understanding with the destination government to ensure that the deportee's human rights were not violated on his return. This is what some other countries seem to have been able to do, at least in some cases.**

c. **To supplement this approach, the Government could seek to establish framework agreements in advance with some of the main countries involved, to minimise the delay in dealing with individual cases. Even if deportation was rarely used in practice in terrorism cases, it might serve to act as a deterrent to international terrorists considering the use of the UK as base for their activities. [Paragraph 254ff]**

29. **From the evidence we have received, we are concerned that there has not been a sufficiently proactive, focused, case management approach to determining whether any particular suspected international terrorist should continue to be detained under Part 4. Nor did it appear that alternative ways of dealing with them were under active consideration. This gap should be filled in time for the first sequence of post-appeal reviews. [Paragraph 200]**

30. **The Government should publish up-to-date anonymised information on its terrorism website on:**

a. **each Part 4 certification setting out its duration and current status, including the outcome of any appearance before the Special Immigration Appeals Commission including bail hearings or appeals (giving both the determination and a link to the full open reasons); and**

b. **the number of detentions that there have been under the Terrorism Acts and their outcomes (e.g., prosecution, certification under Part 4, release). [Paragraph 258]**

Part 5 (Race and Religion)

31. **The case for offences aggravated by religious hatred should be reconsidered in the context of broader mainstream legislation designed to protect the range of targets of hate crime. [Paragraph 267ff]**

Part 6 (Weapons of Mass Destruction)

32. **No objections to this part of the Act have been brought to the Committee's attention. It seems to be an unexceptionable tidying-up of the legislation which in part fulfils our obligations under the UN Biological and Chemical Weapons Conventions. [Paragraph 276]**

Part 7 (Security of Pathogens and Toxins)

33. **Some aspects of Part 7, which was subject to only very limited consultation, need to be urgently addressed.**

    a. **The list of relevant pathogens contained in schedule 5 (the so-called "Australia list") does not include all those materials which are of concern from a counter-terrorist point of view. The list in the Schedule should be amended to include all of these, as recommended by the House of Commons Select Committee on Science and Technology.**

    b. **Evidence to the Committee highlighted security concerns surrounding the holdings of some diagnostic laboratories. They should also be covered by the Act. [Paragraph 294]**

34. **Part 7 is only now beginning to have a direct effect: its further implementation should be subject to regular reporting to the Home Affairs Select Committee. We draw this matter to their attention. [Paragraph 295]**

35. **The security of pathogens and toxins in the post and in transit is being addressed as part of the present inspection and consultation process by counter-terrorist security advisers; where possible, it is desirable that security should be built on the foundation of close consultation and co-operation between inspectors and laboratories. However, evidence to the Committee indicated that there are no relevant security (as opposed to health and safety) regulations for postage and transport; it would be consistent with the rationale for Part 7 of this Act if police counter-terrorist security advisers were given statutory powers to enforce security provisions for the carriage of Schedule 5 pathogens and toxins where necessary. [Paragraph 296]**

Part 8 (Security of Nuclear Industry)

36. **Existing regulations for non-nuclear radioactive sources only allow for the enforcement of health and safety regulations (as with the provision for the handling of pathogens and toxins in laboratories before this Act) and are not designed to prevent intrusion by an individual seeking to use radioactive material with a view to causing deliberate harm. This gap should be filled. [Paragraph 310]**

37. **We believe that the security of radioactive sources should also be the subject of an annual report to Parliament, including information on any losses, and subject to**

further scrutiny by a Select Committee. Responsibility for this area is shared between a number of Departments, and we believe that the House of Commons Science and Technology Committee would probably be the most appropriate. [Paragraph 311]

Part 9 (Aviation Security)

38. **Part 9 provides useful powers for tightening security at airports. They address certain threats to aviation from organised and other crime, including terrorism. They should, therefore, be revisited in the context of wider mainstream transport security legislation when a suitable legislative opportunity arises. [Paragraph 314]**

39. **Urgent consultation with air and ferry operators is required regarding the provision of advance passenger information under Section 119 of the Act. The Government should report during debates on this Committee's report on the steps that it has taken to increase compliance with the legislation. [Paragraph 327ff]**

40. **No fundamental concerns with the present primary legislation for aviation security generally were brought to our attention, but some specific security issues were raised with us. [Paragraph 330]**

    a. **In the light of the attacks of 11th September 2001, extensive attention has been given to controlling the entry of individuals and their hand luggage at points of access to the restricted zone of airports. Less attention has been given to access by cargo and other goods at other points of entry to the zone: for instance, to the checking of security seals placed on vehicles off-site. It is important that the extensive efforts that have been made to enforce security at points of access within the main airport buildings should not be undermined in this way.**

    b. **Lord Carlile commented in his report on the Terrorism Act 2000 on the inadequacies of Special Branch accommodation at some air and ferry ports, resulting in practical difficulties for the interrogation of suspects. We were told that steps were in hand to remedy the space restrictions, but the Committee's visit to Heathrow confirmed that better facilities are still required. This is a matter for the Home Office and airport operators.**

    c. **Police specialising in terrorist and national security operations have experienced difficulties with the new personal search regime which applies to all people with access to the restricted zone, including airline and control staff. It has endangered a number of sensitive operations being conducted by Special Branch officers. It is desirable that all staff should be subject to the regime, but some means of relaxing controls in this very specific category of operations should be devised.**

41. **We draw these matters to the attention of the Transport Select Committee.**

Part 10 (Police Powers)

42. **Most of the reported uses of the Part 10 powers have not been related to counter-terrorism. While some of the measures have intrinsic merit, they should be submitted again when the underlying legislation is next revised. Other provisions present an intrusion into individual rights which are not justified by any counter-terrorist benefits and should either be repealed or significantly amended. [Paragraph 333ff]**

43. **We were struck by the extent to which terrorists use crimes of "identity theft", involving the use of false personal documentation, as a basis for their operations. The falsification of identity documents enables them to evade detection, circumvent immigration controls, and raise funds illegally. This is a serious issue; however, we are not convinced that all the relevant measures in Part 10 address it effectively. [Paragraph 336]**

44. **The privacy of innocent citizens who are subject to the Part 10 procedures should be protected. Those subsections enabling the police to retain fingerprints and photographs should be amended, permitting retention only in circumstances where the subject is charged with an offence, or where appropriate authorisation is given that that they are of ongoing importance in a terrorist investigation. [Paragraph 341ff]**

45. **The Terrorism Act 2000 provided no powers to fingerprint in circumstances where there was a reasonable suspicion of involvement in terrorism, but not of involvement in a specific offence. Section 89 fills that gap. This is an important amendment in view of the role of identity theft in terrorism. The power should however be subject to the same retention safeguards as the parallel powers contained in the Police and Criminal Evidence Act 1984. [Paragraph 346]**

46. **The Section 36 provision that fingerprints taken under immigration powers can be retained for 10 years under all circumstances also gives rise to privacy concerns, and its justification on counter-terrorist grounds is not clear. The previous position on retention of fingerprints should be restored, except where appropriate authorisation is given that the fingerprints are of significance in an ongoing terrorist investigation. [Paragraph 347ff]**

47. **The previous limits on the general circumstances where the police are entitled to demand the removal of disguises should be restored. We are however satisfied that a more strictly defined power should be retained for those cases where a senior police officer believes that this measure is necessary in response to a specific terrorist threat. [Paragraph 353ff]**

48. **It is desirable in the limited circumstances set out in Sections 98 to 101 that constables of the British Transport and Ministry of Defence Police should be able to act with all the authority of "Home Department" constables. We support the extension of the jurisdiction of both forces, but believe that it should be revisited when the underlying legislation is next revised. [Paragraph 362]**

49. **Given the special character of the Ministry of Defence Police it is important that the details of any mutual aid operations should be recorded and reported to Parliament. We welcome the Chief Constable's undertaking to provide an annual operational report in addition to the report and accounts required of him as Chief Executive of the Agency. The report should include detailed information regarding operations undertaken under Section 99. [Paragraph 363ff]**

50. **Future appointments of independent members to the MoD Police Committee (including the representatives of the appropriate trade unions and forces' family associations) should be subject to the Code of Practice of the Commissioner for Public Appointments, including public advertisements of the vacancies. We also take the view that, in the interests of independence, the Chairman of the Committee should also be drawn from outside the armed services and the Ministry of Defence, and the appointment should be subject to the same procedure. [Paragraph 371ff]**

Part 11 (Retention of Communications Data)

51. **We can see the case in principle for requiring communications data to be retained for a minimum period (which would vary with the type of data) for a defined range of public interest purposes such as helping in the prevention and detection of terrorism and other serious crime. These provisions should, therefore, be part of mainstream legislation and not special terrorism legislation. [Paragraph 396]**

52. **The Government should accept the logic of the results of its consultation and replace Part 11 with a mainstream communications data retention regime which limits in primary legislation the longest retention period which the Government can impose to one year. This approach seems to have been adopted in several other European countries. It would permit data which is of potential use in safeguarding national security to be retained. Access to the data must, however, be subject to strict regulation, and that regulation must be properly enforced. [Paragraph 398ff]**

53. **The whole retention and access regime, including for those access routes not governed by the Regulation of Investigatory Powers Act 2000, should be subject to unified oversight by the Information Commissioner. [Paragraph 405]**

54. **The need to retain communications data for terrorism and other serious crimes creates the potential for other use or abuse of that data. The protection provided by the Regulation of Investigatory Powers Act is a step in the right direction where it applies, but a coherent legislative framework governing both retention of, and access to, communications data seems to be the only way of providing a comprehensive solution to this issue. [Paragraph 406]**

55. **Data preservation** (preventing the anonymisation of a specified set of communication data such as that relating to a particular subscriber) **is a useful supplement to data retention, and it should be properly provided for and regulated. [Paragraph 407ff]**

Part 12 (Bribery and Corruption)

56. **We endorse the view of the Joint Committee on the Draft Corruption Bill that a radical simplification of the bribery and corruption law in the forthcoming Corruption Bill would enhance its impact; it would serve as a better basis for prosecution, and send a clearer practical message to those professionals who are most affected by it. [Paragraph 421]**

Part 13 (Miscellaneous)

57. **It is preferable for prosecution to take place on the grounds of direct involvement in terrorism where possible, but we understand that use of the offence of withholding information may be the only way forward in some serious cases. We invite Lord Carlile to keep the operation of Section 117 under particularly careful review. [Paragraph 434]**

Part 14 (Supplemental)

58. **The powers of amendment set out in Section 124 are particularly unwelcome in emergency legislation of this kind, and they should be repealed. [Paragraph 442]**

59. The provisions that we specify under Section 123 are discussed on page 9.

C: Introduction

C.1: The Review

The Anti-terrorism, Crime and Security Act 2001

Purpose

60. In the aftermath of the events of 11th September the Government introduced the Anti-terrorism, Crime and Security Act 2001 to ensure that it had sufficient powers to counter the terrorist threat to the UK. It also contained a range of more generally applicable crime and security provisions.[3]

Scope

Part 4: Immigration and Asylum

61. The most controversial and difficult issue raised by the Act is the way in which it addresses cases where

    a. there is persuasive intelligence, normally from more than one source, that a foreign national has links to terrorist networks linked to al Qaeda, but cannot be prosecuted, either because the intelligence is not admissible in court, or because making it public could put sources at risk; and furthermore

    b. it would be contrary to our international obligations to deport the suspect, normally because there is a risk that they would face inhuman or degrading treatment in any state prepared to take them.

62. The courts have ruled[4] that it is contrary to the right to liberty under Article 5 of the European Convention on Human Rights to detain someone pending deportation if there is no real prospect of actually deporting them. Part 4 of the Act effectively disapplies this ruling (requiring derogation from Article 5) and so provides an immigration-based framework for detaining the narrow group of foreign terrorist suspects who cannot be prosecuted for involvement in al Qaeda-related terrorism and who cannot be deported.

63. This raises a number of general issues (e.g., whether deportation really is the right approach, how the threat from British nationals suspected of involvement in terrorism is addressed, why no other country has found it necessary to derogate from the ECHR to deal with such terrorism) as well as specific issues relating to the fairness of the appeal and review procedure governing detention.[5]

64. The detention powers under Part 4 need to be renewed by Parliament at least annually, until 10th November 2006, when they expire. Lord Carlile of Berriew QC reviews the operation[6] of Part 4 periodically.

Other provisions

65. The Act is broad in scope, also covering:

[3] Anti-terrorism, Crime and Security Act 2001, Explanatory Notes, page 1.
[4] *Chahal v United Kingdom* (1996) 23 EHRR.
[5] We discuss these in detail under Part 4, page 52ff.
[6] Under Section 28 of the Anti-terrorism, Crime and Security Act 2001.

a. a strengthening and extension of the powers available in the Terrorism Act 2000 (e.g., enhancing its provisions for investigating terrorist property, and making failure to disclose information about acts of terrorism a criminal offence). Building on Lord Lloyd of Berwick's report *Inquiry into Legislation Against Terrorism,*[7] the Terrorism Act 2000 was intended to put counter-terrorism legislation largely on a permanent basis with application not only to Irish terrorism, as had been the main focus hitherto, but also to other international and domestic threats. Lord Carlile of Berriew QC reviews the working of the Terrorism Act 2000 annually. The Committee has kept in touch with Lord Carlile and worked closely with him on those parts of the Anti-terrorism, Crime and Security Act 2001 that modify the Terrorism Act 2000;

b. updated and strengthened regulatory frameworks for the civil nuclear industry, and for the control of pathogens and toxins and offences relating to weapons of mass destruction and other dangerous substances;

c. a range of traditional investigatory and procedural material covering, for example, the disclosure by public bodies of information such as addresses to assist investigations and prosecutions, security at airports, the retention of communications data by phone companies and internet services providers, as well as the rules about fingerprinting, and extending the jurisdiction of the MoD Police and British Transport Police;

d. a measure increasing the sentences for certain crimes when they are motivated by religious hostility;

e. a (now lapsed) measure to allow the transposition of EU police and criminal judicial co-operation measures into UK law by secondary, rather than primary, legislation.

The Review

Remit

66. The Act had an accelerated passage through Parliament, and there was Parliamentary pressure for the duration of the legislation to be limited. The Government conceded that the controversial detention provisions and the communications data provisions should contain "sunset clauses". Instead of time limiting the rest of the Act, the Government agreed[8] to establish a Committee of at least seven Privy Counsellors to review the whole Act by 13th December 2003. The Committee's report was to be submitted to the Home Secretary, who was required to lay it before Parliament as soon as reasonably practicable.

67. The Committee was empowered to specify provisions of the Act, which would be repealed if the Report was not debated by each House of Parliament within 6 months. This remit is discussed on page 9.

68. The review was given no specific terms of reference, but its remit is set out in Sections 122 and 123 of the Act.[9]

[7] Cm 3420, published in October 1996.
[8] See page 106ff for the Parliamentary debate on this concession.
[9] See Annex E.3: page 106 for more details.

The Committee

69. The Home Secretary, the Rt. Hon David Blunkett, MP, appointed the Committee members in April 2002 saying:

> *I made clear to Parliament during the passage of the Act that effective independent scrutiny is an important part of its working effectively. The Review committee will provide independent parliamentary oversight of the operation of the Act and I am very grateful to all the Privy Counsellors who have agreed to join and carry out this important work on behalf of Parliament and the people. I am particularly grateful to Lord Newton who will chair the committee, having earned the respect and trust of members of Parliament during his many years' service in both houses.*

70. The Committee Members appointed were:[10]

- The Rt. Hon Lord Newton of Braintree (Chairman)
- The Rt. Hon Alan Beith, MP (Deputy Chairman)
- The Rt. Hon The Lord Browne-Wilkinson
- The Rt. Hon Terry Davis, MP
- The Rt. Hon Baroness Hayman
- The Rt. Hon Lord Holme of Cheltenham
- The Rt. Hon Sir Brian Mawhinney, MP
- The Rt. Hon Joyce Quin, MP
- The Rt. Hon Dr Chris Smith, MP

71. On appointment, Lord Newton of Braintree said:

> *This Act, passed after the World Trade Center attack last year, contains very significant powers. People both inside and outside Parliament need to be confident they strike a proper balance and are appropriately used. Reviewing it, and making proposals for the future is an important task. I am pleased to have been asked to play a part, and to be supported by so strong a group of fellow Privy Counsellors.*

Approach

72. In conducting our review, we have sought to take evidence both from those relying on the Act's powers, such as the police and security services, and those with views on their use, including a range of academics, lawyers and organisations with an interest in the field.

73. Since July 2002 the whole Committee has met 22 times either to take evidence or for discussion and undertaken 18 visits in smaller groups, plus a number of individual visits by Committee Members and the Secretariat. The groups and individuals who have contributed to the review are listed on page 111ff. In addition to the material that we

[10] For further details about the Committee members see page 114ff.

received from them, we have seen a wide range of written material such as House of Commons Library papers, legal judgements, academic papers, reports by earlier reviewers of this and other legislation, including Parliamentary Select Committees, and have followed press reports and comment. We have also tried to take account of debates which have been in progress during the course of our Review, such as those on the continuation of Part 4, on communications data retention and access, on religious offences, and on bribery and corruption.

74. We have seen a small sample of the "closed" material on the basis of which the suspected international terrorists have been detained; we have attended both open and closed sessions of the Special Immigration Appeals Commission and visited the prisons holding the detainees.

75. We have not, however, sought to duplicate the work of the courts or of the Special Immigration Appeals Commission by seeking to form judgements on the compatibility of the Act with the UK's international obligations and other legislation such as the Human Rights Act, or considering the merits of individual cases. We have also tried to avoid duplicating the work of Lord Carlile of Berriew on the operation of Part 4 of the Act.

This Report

76. The following chapter of the report makes some general observations on individual rights and public safety. We then set out the basic principles which, in our view, should govern counter-terrorism legislation (page 28ff).

77. The main section of the Report covers the Act itself, Part by Part (page 34ff).

78. A summary of our main conclusions is set out on page 8ff. A synthesis of our specific recommendations can be found on page 10ff.

C.2: Individual rights and public safety

The threat from terrorism

79. Although there is no universally accepted definition of terrorism,[11] it encompasses the tactic of using violence against public institutions and the population at large to achieve political ends.

80. Terrorism operates by spreading fear, undermining morale and causing disruption. The threat of terrorism contributes to these ends, and terrorists exploit the psychological impact of their attacks or the threat of them which in contemporary society is magnified by media exposure. Because it seeks to challenge the integrity of normal life, it is inevitable that society will seek the appropriate means to protect itself.

The duty of the state

81. The state has a duty to protect the public from harm, even at the expense of some individual rights. After all, terrorists curtail the rights of those affected by their activities. Aspects of this obligation are codified in international law. For example, Articles 1 and 2 of the European Convention on Human Rights, in combination, require the state to ensure that "Everyone's right to life shall be protected by law".

82. Some of the terrorist networks that pose the greatest risk to the public are transnational in nature.[12] The authorities need, therefore, to co-operate closely with their counterparts in other countries as an essential component of the response to the threat from such networks. The importance of this point was emphasised to us in evidence from foreign law enforcement practitioners.

[11] There are broadly two points of view. One is that violence against the public and against public institutions is terrorism, irrespective of the merits of the objectives of the perpetrators, and the other is that it is possible to distinguish terrorists from "freedom fighters" – those pursing the right to self-determination in societies where there are no legitimate means of securing change – by the merits of their objectives. The definition of "terrorism" in Section 20(1) of the Prevention of Terrorism (Temporary Provisions) Act 1989 was "the use of violence for political ends and includes any use of violence for the purpose of putting the public or any section of the public in fear." The definition in Section 1 of the Terrorism Act 2000 is longer, covering more explicitly single-issue or religious terrorism and terrorism involving damage to property, or disruption of electronic systems. It is expressed in terms of *serious* violence. An additional approach is to define terrorists through their connection with groups which have been proscribed as terrorist organisations. Under the Terrorism Act 2000, organisations can appeal against their proscription to the Proscribed Organisations Appeal Commission, which uses procedures similar to those of the Special Immigration Appeals Commission used in Part 4 of this Act. For a European definition of terrorism, see page 119. The United Nations has defined terrorism implicitly, in terms of the methods used by terrorists. (See UNSCR 1373.)

[12] See, for example, the description of the various groups in paragraphs 119ff of the "generic evidence" section of the generic Special Immigration Appeals Commission judgements on Appeals SC/1,6,7,9,10/2002 of 29th October 2003.

83. It is in the nature of terrorism that it is impossible to prevent it completely.[13] Self-evidently, the most effective way of dealing with terrorists is to pre-empt their activities (by closing off opportunities for terrorist action through vigilance and the effective use of intelligence, by making it difficult for them to communicate, and by cutting off their access to funding and other resources) or to prosecute them. It is important to accomplish this in a way that is effective and does not represent a worse curtailment of the rights of the individual than the threat that it seeks to address. A body of law giving the state proportionate powers, subject to proper safeguards, is, therefore, essential. (We discuss our preference for more intensive use of surveillance over the use of the detention powers of Part 4 of the Act on page 65.)

The need to limit counter-terrorism powers

84. The authorities are not infallible so their powers must include limitations and safeguards to reduce the danger that they could be misapplied. Misuse of such powers:

    a. results (by definition) in individual cases of injustice or harm;

    b. leads to a false sense of security (because the actual terrorists are still going about their business);

    c. brings the use of those powers into disrepute (undermining the case for their use where they are genuinely needed to protect the public).

85. A recent example that risks falling into the latter category has been the use of Section 44 of the Terrorism Act 2000 to search protesters outside the Arms Fair at the Excel Centre in Docklands in October 2003.[14] Normally there are safeguards against the misapplication of intrusive powers such as appeal procedures, or external oversight, or the need for judicial or Ministerial approval before they are used. The latter may not be adequate if the exercise of the powers is not apparent and so the Minister's answerability to Parliament and to the public for acceding to their use is only theoretical. For example, it only emerged during the court hearing on the application of Section 44 of the Terrorism Act 2000 to Docklands Arms Fair protesters that the powers have been renewed every 28 days since the Act came into force in February 2001, and are still in force across London. They have also been used in almost every other police area in

---

[13] The Home Secretary, David Blunkett, speaking on the BBC's Today programme in November 2003 said: "It's very good intelligence that actually saves you in the end, not massive concrete blocks around every piece of British territory abroad or for that matter all our iconic buildings. We have police, and we have security where it's appropriate.
"We get criticised for pulling those police out of the neighbourhoods and communities so we've got to get a balance here between common sense. It won't be people standing about waiting for suicide bombers that will save us, it will be very, very good intelligence."

[14] This use aroused controversy, but was upheld by the High Court in the case 2003 EWHC 2545 (Admin). Lord Justice Brooke and Mr Justice Maurice Kay had no hesitation in concluding that the judicial function in scrutinising a decision of this kind was necessarily a limited one. The assessment of the risk to public safety and to national security and the formulation of measures to safeguard the public and national security were primarily for the Government and Parliament on grounds of political legitimacy (see *Home Secretary v Rehman* [2001] UKHL at [62]; 2003 1 AC 1534: compare *R (ProLife) v BBC* [2003] UKHL 23 at [76]; 2003 2 WLR 1403). A senior police officer with major operational responsibility had made the authorisation, and the Home Secretary, who had wide sources of relevant expertise available to him and was answerable to Parliament, had confirmed it. In their judgment it was within their powers to make this authorisation and to confirm it, and there were no grounds on which they should set it aside as a matter of law.
There had been just enough evidence available to persuade the judges that "in the absence of any evidence that these powers were being habitually used on occasions which might represent symbolic targets, the arms fair was an occasion which concerned the police sufficiently to persuade them that the use of section 44 powers was needed. But it had been a fairly close call."

Britain (though it has not been made public whether they have been continuously renewed outside the capital). Had Parliament envisaged such extensive and routine use of these powers, it might well have provided for different safeguards over their use. We have drawn these points to the attention of Lord Carlile of Berriew, who reviews the working of the Terrorism Act 2000. Similar issues have recently been raised in relation to the draft Civil Contingencies Bill.[15]

86. It is an important principle of our legal system that a person should be liable for arrest only when they are suspected of having committed (or of being about to commit) a specific crime. Counter-terrorist powers are, therefore, more likely to interfere with the rights of the individual than conventional police powers because they seek to pre-empt terrorism, that is to allow intervention before a specific crime has taken place, as well as to punish crimes after the event.

87. Giving the authorities untrammelled powers to exercise against suspected terrorists may seem reasonable in the heat of the moment, until they are exercised against the wrong people (perhaps through mistaken identity rather than mischief) and those at the wrong end of them find that the procedures for redress are inadequate.[16] The case of the 72-year-old British man held in a South African prison for nearly three weeks in an identity mix-up by the FBI earlier this year illustrates the point in a non-terrorist context.[17]

88. Neither do more extensive powers always lead to greater public safety. The East German Government may have had files on a quarter of their population, but it failed to predict or prevent its own demise. If there is too much information, it can be difficult to analyse effectively and so can generate more leads than can be followed up or trigger too many

[15] The draft was published as Cm 5843, in June 2003. See the Report of the Joint Committee on the Draft Civil Contingencies Bill, Session 2002-03, Report and Evidence, 39-50.

[16] Cases of administrative error are almost inevitable. For example, in the ten Special Immigration Appeals Commission judgments handed down on 29th October the judges observe that "While not central to any issue arising in this appeal, it is a matter of concern that [a factual error] should have occurred." (in the case of Abu Rideh), "the grant of refugee status [to C] was an error", "There has been confusion about [D's] immigration history, because of a typographical error in one of the statements, an allegation made against him which resulted in his arrest and release in 1999, and, apparently as a result, duplication of bail records.", "The 2001 Act came into force in December 2001, but [H] was not certified or detained until 22nd April 2002. In his statement, he expresses bewilderment that he should be considered a risk to national security at all, but greater bewilderment that he should have been detained in April 2002 rather than December 2001. The answer to the delay in certifying lies, according to witness A, in the loss of one of his files and the view that it would be wrong to proceed against him in its absence. We see no reason to reject that evidence although we are bound to express some concern that someone who was considered and, as we have concluded, correctly considered to be a danger to national security should have been left at large because a file had gone missing." While such errors may have been inconsequential, they illustrate the need for safeguards to deal with cases where they are not.
For a further example of the type of error that can occur in practice, which again the procedures picked up, see http://foi.missouri.edu/secretcourts/seccrtrebuffs.html for a report of a legal ruling relating to the mishandling of search warrant and wiretap applications.

[17] Mr Derek Bond is reported as saying that nobody took a personal statement from him until he had spent 10 days in the police cells. He was only released after an anonymous tip-off to the FBI after media coverage of the case, which led to another man being arrested in Las Vegas. It took a further 12 hours after that arrest for all the formalities to be completed to allow Mr Bond to be released.

false alarms.[18] Sophisticated terrorists change their profile and methods to avoid presenting a static target. For example, al Qaeda is reported to place particular value on recruiting Muslim converts because they judge them to be less likely to be scrutinised by the authorities.[19]

89. The rights of the individual and the needs of security must both be met. There will always be a tension between them, and the rights of the individual should be curtailed only after the most careful consideration. Extensions to the powers of the state in securing the safety of its people should always be tested rigorously for both necessity (which encompasses proportionality) and effectiveness. Where such powers pass this stringent test, they must in any case be subject to proper safeguards against misuse (whether deliberate or not) such as special procedures for authorising their use, periodic review and renewal, regular reporting of usage, independent oversight, and exercisable rights of appeal and redress for the individual. Additional safeguards are particularly important in the context of counter-terrorism powers because the courts, which might otherwise provide a check on their use, tend to see the assessment of the risk to public safety and to national security and the formulation of measures to safeguard the public and national security as primarily matters for the Government and Parliament on grounds of political legitimacy.

90. This may seem straightforward, but can give rise to some difficult questions in practice. For example, would it be acceptable to use torture on terrorist suspects in cases where it might help to save lives, to take a deliberately extreme case? A democratic society cannot act with the freedom from restraint and lack of ethical principles that are open to terrorists. While this can be characterised as fighting terrorism with one hand tied behind our backs, the rule of law and a proper respect for individual liberties are themselves important elements of security.[20]

Guiding principles

91. These observations can be summarised in the following principles set out by Lord Falconer of Thoroton QC, which we endorse:[21]

[18] This was, arguably, the flaw in Admiral Poindexter's Total (later Terrorist) Information Awareness (TIA) initiative, a proposed data mining system intended to identify potential terrorists and criminals by trawling financial records, medical, communication, and travel records and intelligence data. But there are easier ways of finding trainee pilots if you know that is what you are looking for and if you do not, a search engine will not help you. Such a facility would, however, create opportunities for criminals to steal personal data. It would, therefore, not only be useless, it would be harmful. (See Bruce Schneier, *Beyond Fear: thinking sensibly about security in an uncertain world*). The Suspicious Activity Reporting regime for financial transactions was criticised by KPMG for its low signal to noise ratio ("over-reporting"). See paragraph 134ff for further details.

[19] For example, Pierre Robert is reported as being behind the May 2003 bombings in Casablanca, and Christian Ganczarski has been charged for his alleged role in the 2002 Djerba synagogue attack.

[20] For a fuller discussion of these issues in the context of a real case, see *A Judge on Judging: The Role of a Supreme Court in a Democracy*, Harvard Law Review, Volume 116, Number 1, November 2002, page 148ff.

[21] House of Lords Debates: 26 March 2003, cols. 851-4:

> *First, our society is based on the liberty of the individual. It is what we fight to protect where necessary. Our starting point, therefore, in a free democratic society, must be that the liberty of the individual should not be limited unless a proper case for limitation is established. Plainly, threats to national security can form the basis of such a case, but only on the basis that the threat to liberty which the threat to national security poses justifies that limitation of liberty... At all stages, one must be careful to ensure that the limitation one imposes, either permanently or in the face of an actual threat, is proportionate to the threat which is posed.*
>
> *...*
>
> *Let me suggest a number of other principles. Any limitations on individual freedom must be proportionate to the threat; they must be sanctioned by law and cannot take place on an ad hoc basis; and they must be implemented in a way which ensures that there are safeguards and that the activities of the executive are subject to monitoring, scrutiny and accountability. If limitations are implemented excessively, the framework must ensure that the monitoring, scrutiny and accountability arrangements are likely to identify and remedy such excesses. In other words, if protections are put in place they must be effective.*

C.3: Legislation against terrorism

Principles governing legislation against terrorism

92. In 1996, the Rt Hon Lord Lloyd of Berwick set out four principles governing special legislation against terrorism:[22]

    a. legislation against terrorism should approximate as closely as possible to the ordinary criminal law and procedure;[23]

    b. additional statutory offences and powers may be justified, but only if they are necessary to meet the anticipated threat. They must then strike the right balance between the needs of security and the rights and liberties of the individual;

    c. the need for additional safeguards should be considered alongside additional powers; and

    d. the law should comply with the UK's obligations in international law.

93. Lord Lloyd described these principles in terms of their implications for the Prevention of Terrorism Act 1974 and the Police and Criminal Evidence Act 1984.

94. We believe that these objectives continue to provide a useful framework within which to analyse legislation against terrorism for the reasons set out in the previous section.

95. In addition to considering the extent to which the measures in the Anti-terrorism, Crime and Security Act 2001 meet Lord Lloyd's principles, the Committee has tried to identify for each Part of the Act:

    a. Scope – whether the measure

        i. is focused exclusively on terrorism or whether it is a mainstream measure that may be applied in terrorism cases among other crimes; and whether it

        ii. matches the extent of the problem that it is intended to address;

    b. Efficacy – how well the measure "works". This covers such matters as

        i. whether it is "fit for purpose";

        ii. whether it contains adequate safeguards of the rights of the individual;

        iii. the number of times that it has been used;

        iv. what has been achieved through its use;

        v. an assessment of the way in which it is used in practice;

    c. What conclusions we should draw. For example:

[22] Chapter 3 of *Inquiry into Legislation Against Terrorism*, (Cm 3420), October 1996.

[23] That is to say, it should depart from the normal criminal law only where this can be shown to be necessary and proportionate to the need.

i. whether the measure should be continued;

ii. whether it should form part of the special counter-terrorism legislation that we envisage;

iii. whether it should be reconsidered in the context of mainstream legislation;

iv. whether there are possible preferable alternatives which should be given further consideration.

Special counter-terrorism legislation

96. Terrorism involves the commission of serious crimes and ought, where possible, to be prosecuted through normal legal processes. In some circumstances, it may be appropriate to differentiate between the maximum sentence available for a crime depending on whether its purpose is terrorism or, for example, self-enrichment. As well as limiting the effect on civil liberties, the use of mainstream processes avoids giving terrorists any special status. However, experience shows that these processes are not always sufficient.

97. The Lloyd Review[24] saw a continuing need for specialist counter-terrorist legislation, essentially because:

a. the techniques used by terrorists make them more difficult to catch and convict than other criminals without additional offences and additional powers for the police and security services; and because

b. terrorists pose a particularly serious threat to society. A longer prison sentence may, therefore, be appropriate for a crime committed in pursuit of a terrorist cause. In addition, special pre-emptive powers may be justified (such as the powers of arrest created by the Terrorism Act 2000[25]).

98. We think that that judgment remains valid today and, if anything, the case for such legislation is stronger. Technological progress and the greater interconnectedness of society mean that terrorists can inflict greater damage. The greater ease of communication makes it easier for them to operate internationally, which makes them harder to catch. Some have little or no regard for their own lives or welfare, which makes them harder to deter.

The Terrorism Act 2000

99. The UK has long had special legislation to deal with terrorism.[26] The Terrorism Act 2000, which followed Lord Lloyd's review, was intended to modernise and streamline legislation on terrorism, adapting it to the then emerging threat of international terrorism and in the light of developments in Northern Ireland, and to provide a settled legislative framework for dealing with terrorism.

[24] *Inquiry into Legislation against Terrorism*, (Cm 3420), October 1996, page 23.
[25] Under Section 41, the police may arrest a person without warrant on suspicion of their being a terrorist, unlike in ordinary arrests where grounds for suspecting involvement in a specific crime is necessary.
[26] A history of UK legislation is given in the introduction to *Blackstone's Guide to the Anti-Terrorism Legislation*, by Professor Clive Walker.

100. In common with a number of other countries,[27] the UK introduced a piece of wide-ranging legislation intended to strengthen the Government's ability to counter the threat from terrorism after the unprecedented attacks in the USA on 11th September 2001, namely the Anti-terrorism, Crime and Security Act 2001.

101. Nevertheless, the Terrorism Act 2000 has continued to provide a sound core for counter terrorist investigations and prosecutions since the events of 2001,[28] and it was necessary to introduce relatively few new specific counter-terrorist measures in the 2001 Act.[29]

The need for durable legislation against terrorism

102. Attacks in Bali (October 2002), Mombasa (November 2002), Riyadh (May 2003), Casablanca (May 2003), and Istanbul (November 2003), for example, and attempted bombings in several other countries have demonstrated that the threat from terrorism around the world is a continuing one.

103. The Director-General of the Security Service, Eliza Manningham-Buller, has commented:[30]

> *We are now past the second anniversary of the terrorist attacks on the United States, and it is clear that the threat from Islamist terrorism will be with us for a long time. I see no prospect of a significant reduction in the threat posed to the UK and its interests from Islamist terrorism over the next five years, and I fear for a considerable number of years thereafter.*

104. The terrorists have not had it all their own way; there have been arrests and convictions for terrorism in countries such as Belgium,[31] France, [32] Germany,[33] Italy,[34] Spain,[35] the

[27] For instance, comparable legislation was also presented in Autumn 2001 in Canada (the *Anti-Terrorism Act 2001*); the United States (the *USA PATRIOT Act*); France (*la Loi sur la Sécurité Quotidienne*); and Germany (*Das Terrorismusbekämpfungsgesetz*).

[28] For instance, between 1st November 2001 and 4th November 2003 there were 281 investigations under the Terrorism Act 2000, as opposed to 17 certifications under Part 4 of the Anti-terrorism, Crime and Security Act 2001. 34 of these investigations resulted in charges under the 2000 Act.

[29] Amendments to the Terrorism Act were made under Parts 1, 10 and 13.

[30] James Smart lecture, 16th October 2003.

[31] On 30th September 2003 a Belgian court sentenced Nizar ben Abdelaziz Trabelsi, an al Qaeda operative, to 10 years in prison for plotting a suicide attack on a NATO base in Belgium. Nine other people also received sentences in connection with the plot. The Brussels Criminal Court sentenced the 10 men for their roles in a passport forgery ring that played a part in the assassination of an Afghan rebel leader in September 2001.

[32] France has a history of extreme Islamist terrorism. For example the Algerian Armed Islamic Group (GIA) killed 8 and wounded 150 on 25th July 1995 in a bomb attack on the Paris Métro.

[33] For example, a 29-year-old Moroccan student Mounir al Motassadeq was convicted in Hamburg in February 2003 on charges including accessory to murder in relation to the 3,045 people killed in the US attacks, membership of a terrorist organisation, attempted murder and five cases of causing grievous bodily injury. A defence motion for the release of Abdelghani Mzoudi (who had been arrested on similar charges) was granted in December 2003 after investigators informed the court of new testimony. In Frankfurt in March 2003, four Algerians accused of plotting to bomb the Strasbourg Christmas market in France on New Year's Eve in 2000, were convicted of conspiring to plant a bomb and of weapons violations and sentenced to prison terms of between 10 and 12 years. Prosecutors had claimed the defendants were part of a network of predominantly North African extremists called the Non-aligned Mojahedin, with ties to al Qaeda. The *Guardian* newspaper has claimed that the tipoff which led to their arrests followed the interception by British intelligence of a telephone call by one of the plotters to "Abu Doha", an Algerian charged in the US with masterminding a plot to blow up the Los Angeles airport. He is currently imprisoned in the UK facing extradition proceedings to the US.

USA[36] as well as the UK.[37] Nevertheless, detecting and countering terrorism presents a formidable practical challenge for the authorities, and it would be prudent to assume that the threat from terrorism will not diminish. We need, therefore, to ensure that we have in place properly considered long-term measures to counter it and that those measures command public support.

105. This was the Government's aim when it brought in the Terrorism Act 2000. The Government's consultation paper preceding the Act said:[38]

> *"The Government is committed to changing the climate in which terrorists operate. It recognises that the threat from international terrorist groups (and to a lesser extent other groups within this country) means that permanent UK-wide counter-terrorist legislation will be necessary even when there is a lasting peace in Northern Ireland. And it also recognises that proposals for new legislation must take account of the fact that the nature of terrorism is ever changing with new methods and technologies being deployed within and across national boundaries …*
>
> *Terrorism is a global threat and international co-operation is essential to counter it. Lessons can be, and have been, learnt from the experience of other governments, and the UK and other governments and their agencies will need increasingly to exchange information and expertise in helping one another combat terrorism. …*
>
> *The Government's aim is to create legislation which is both effective and proportionate to the threat which the United Kingdom faces from all forms of terrorism — Irish, international and domestic — which is sufficiently flexible to respond to a changing threat, which ensures that individual rights are protected and which fulfils the United Kingdom's international commitments…"*

106. We strongly support these objectives.

Legislating in emergencies

107. Terrorists play on the public's difficulty of assessing the risk of an attack. This leads to pressures on the authorities to be seen to be doing something (to make the public feel safer, even if the real threat is not always addressed). If there is a further attack, the authorities will be judged less harshly if they did something, even if it was ineffective, irrelevant, disproportionate or perhaps even harmful, than if they did nothing. The same pressures on the authorities can make it even more difficult to repeal superfluous or

---

[34] For example in March 2002 Essid Sami Ben Khemais, suspected of arranging logistics in Europe for Osama bin Laden, pleaded guilty to charges that included criminal conspiracy to obtain and transport arms, explosives and chemicals, and was sentenced to five years in prison. Three other Tunisians who were tried with him—Belgacem Mohamed Ben Aouadi, Bouchoucha Mokhtar and Charaabi Tarek—were convicted on the same charges and sentenced to prison terms of up to five years. They also fabricated false documents which allowed al Qaeda operatives to travel in Europe and elsewhere. The Tunisians requested and received a fast-track trial, reducing the maximum sentence of nine years to six.

[35] For example, in September 2003 Judge Baltasar Garzon ordered four suspected al Qaeda members to remain in jail following their arrests a day after Garzon issued a 700-page indictment against 35 other people, including al Qaeda leader Osama bin Laden. At least eight of the 35 have been linked to the September 11, 2001, attacks on New York and Washington.

[36] For example, Richard Reid (the "shoe bomber") was sentenced to life plus 30 years in prison in January 2003. See http://news.findlaw.com/legalnews/us/terrorism/cases/index.html for comprehensive details of recent US terrorism cases.

[37] For example, on 1st April 2003 Brahim Benmerzouga and Baghdad Meziane, were jailed for 11 years each by Leicester Crown court after they were found guilty of helping to fund Osama bin Laden's network.

[38] *Legislation against Terrorism*, Cm 4178, December 1998.

ineffective legislation than to enact it. This reinforces the case for allowing the authorities to resort to an existing body of considered, properly regulated, counter-terrorism legislation.

108. We recognise that even with access to such powers, Governments may, from time to time, need to legislate rapidly to protect the public from new threats. Under such circumstances, there is, almost by definition, a risk that the legislation in question will be less well prepared than other law, although it can prove just as durable.[39] Parliament has, over the years, insisted on a range of safeguards in such circumstances, particularly for controversial powers:

    a. time limitation ("sunsetting");

    b. periodic Parliamentary scrutiny and renewal;

    c. independent review or authorisation of the use of the powers.

109. We welcome the limitations on the duration of some of the provisions included in Parts 4, 11, and 13 of the Anti-terrorism, Crime and Security Act 2001. We also welcome the provision that the detention provisions in Part 4 in particular are subject to ongoing periodic independent review and renewal by Parliament. The role of our own Committee has, to some extent, fulfilled the need for independent review for the Act as a whole. However, except for a power to specify which provisions should be repealed should our report not be debated by both Houses of Parliament within six months of publication, our powers are those of persuasion only.

110. Other parts of the Act are of a more permanent character. In many cases these are mainstream provisions, directed at crime in general, rather than terrorism specifically. No matter what their intrinsic merits may be, we believe that they would in general benefit from full and proper consideration in their natural legislative context as opportunities arise. In some cases this is already happening: the Proceeds of Crime Act 2002 has incidentally broadened some of the measures created under the Terrorism Act and amended by the Anti-terrorism, Crime and Security Act 2001[40] (such as the requirement on the financial sector to report suspicious transactions). It is welcome that Part 12 is to be repealed and reconsidered in the context of a wider Corruption Bill. Several other areas of the Act would benefit from similar scrutiny in their normal legislative context.

Special counter-terrorism legislation should not be mixed with mainstream legislation

111. We think that it is an important principle that when we need special counter-terrorist legislation that provides for additional powers or departs from ordinary judicial procedures it should be kept separate from the body of mainstream crime and security legislation. This approach limits the impact on civil liberties and more readily allows for tailored safeguards and penalties to be provided.

112. If a power is narrowly focused on terrorism, it may be appropriate to allow some relaxation of the safeguards that relate to its application, combined with reinforced post-application safeguards.

[39] For instance, aspects of the Prevention of Terrorism (Temporary Provisions) Act 1974 still exist in the form of provisions of the Terrorism Act 2000; the Prevention of Violence (Temporary Provisions) Act 1939 stayed in force for 15 years despite the end of the IRA mainland bombing campaign to which it was directed.
[40] But has not directly amended or replaced them.

113. During the passage of the Act, the Government argued that limiting the application of particular provisions to terrorist crimes was inappropriate, because it could be difficult in practice to distinguish terrorist crimes from other crimes and so the powers in question should be available for all crimes. Even were we to accept this argument (which was not emphasised to us during any of our evidence sessions), its limitations became clear to us when we discovered that some provisions of this Act had principally been used in cases clearly unrelated to terrorism, including sex offences and football hooliganism.

114. Mixing demonstrably urgent counter-terrorism measures with mainstream ones risks undermining the consensus for showing deference to the judgement of the government in emergencies.

115. **The idea of a durable body of properly considered, principled, counter-terrorist legislation – which is distinct from mainstream criminal law, addresses this particular threat to society and includes adequate safeguards of the rights of the individual – remains compelling. This was the Government's stated objective when it introduced the Terrorism Act 2000, and it is the approach to which, in our view, the Government should return.**

D: The Anti-terrorism, Crime and Security Act 2001

D.1: Part 1 – Terrorist Property

Background

116. Terrorist finance presents particular challenges for law enforcement. The funds in question may not derive from illegal activities; the sums involved can be small,[41] and the individuals who use those funds may avoid conspicuously expensive lifestyles in seeking to retain effective cover for their operations.[42] Nevertheless, significant prosecutions in the UK and abroad[43] have illustrated that this is a useful point of intervention in disrupting the planning of terrorist actions before they occur.

117. Most of the provisions in Part 1 derive from the Terrorism Act 2000 which drew on earlier legislation directed at drug trafficking and money laundering. They include provisions for the seizure and forfeiture of funds through civil proceedings without the need for a criminal prosecution, and the obligation that it imposes on the financial sector to report suspicious transactions. This Part makes no fundamental changes to the framework of criminal law set out in the Terrorism Act, but amends it in points of detail.

118. Legislation in this field increasingly follows internationally agreed standards of best practice. Since the attacks of 2001, these have to some extent been standardised both through United Nations Security Council Resolution 1373 on terrorism (passed 28th September 2001), and through the special recommendations on terrorist finance which have been set out by the international Financial Action Task Force.[44]

---

[41] The Treasury estimates that the Bishopsgate bomb in the City of London, which caused damage estimated at £1 billion, cost only £3,000 to mount: *Combating the finance of terrorism: a report on UK action*, October 2002, page 11. The rise of suicide bombing has significantly reduced the material resources required for large-scale attacks; as one recent commentator notes: "…A cost-benefit analysis shows suicide operations to be by far the most efficient form of terror attacks from a military point of view; they require relatively small amounts of money and can have a great impact in terms of casualties and damage. Bin Laden and his followers are well aware of these advantages. According to the head of Egyptian Islamic Jihad, Dr Ayman Al-Zawarahiri, 'the method of martyrdom operation [is] the most successful way of inflicting damage against the opponent and the least costly to the Mujahedin in terms of casualties.' [The 11th September attacks] were the most cost-effective terror attack ever carried out: only 19 hijackers and a budget estimated at $500,000 were employed to kill almost 3,000 people and inflict a permanent scar on Western society," Loretta Napoleoni, *Modern Jihad: tracing the dollars behind the terror networks*, page 133. It has been suggested that the cost of transporting a terrorist from the UK and equipping him for action in Iraq is about $2,000; *The Economist,* 20th November 2003.

[42] A training manual found by the Manchester police during the search of an al Qaeda member's home contained detailed advice on avoiding the police's attention: for instance, "One should possess the proper [driving] permit and not violate traffic rules in order to avoid trouble with the police"; and, "not [cause] any trouble in the neighbourhood where he lives or at the place of work". A full set of extracts can be found at www.usdoj.gov/ag/trainingmanual.htm.

[43] For instance, a group were successfully prosecuted in North Carolina in 2002 on the basis of providing material support to terrorism through cigarette smuggling and credit card fraud; a ring dealing in credit card fraud for similar purposes was convicted in Leicester in April 2003. See also the Northern Ireland Select Committee's report on *The Financing of Terrorism in Northern Ireland* HC 978-I, 26th June 2002.

[44] The Financial Action Task Force has made recommendations on money laundering since its creation in 1989, when it was founded on the initiative of the G-7 Heads of State and President of the European Commission. 40 countries are members. The Task Force's special terrorism recommendations were issued in October 2001.

119. Following the Terrorism Act and shortly forthcoming regulations, the United Kingdom meets the legislative requirements set by both bodies, and a similar framework also applies in many other countries.[45]

Provisions

120. The Terrorism Act introduced a number of special provisions for the detection and prosecution of terrorist finance. For instance, it:

    a. provided for the seizure and subsequent forfeiture of cash at borders by the police;

    b. required individuals to report activity which came to light in the conduct of their profession and which aroused suspicion of terrorism;

    c. allowed the police to place a "disclosure order" on a financial institution, requiring the release of customer information as part of a terrorist investigation.

121. The Anti-terrorism, Crime and Security Act 2001 amended this framework. Most importantly:

    a. it allows the police to seize cash throughout the United Kingdom;

    b. it creates an objective test of whether a financial institution[46] had been negligent in failing to report a transaction which could reasonably be regarded as suspicious;

    c. it extends the range of information that the police can request from financial institutions.

Our view

122. In our view, the amendments made by Part 1 and its Schedules are a proportionate and effective extension of the framework set by the Terrorism Act 2000. We have some recommendations on their implementation.

Cash seizures

Usage

123. The cash seizure power under Schedule 1, Part 2, has been used (as at 15th October 2003) on 18 occasions, leading to the seizure of over £270,000.

Our view

124. **Schedule 1 extends the power of the police to seize 'terrorist cash' at the borders (and pursue its eventual forfeiture through civil proceedings) throughout the United**

[45] For instance, the requirement to report suspicious transactions, which is one of the FATF requirements, applies in the United States and other countries. The USA PATRIOT Act extended an existing reporting requirement to money service businesses and other categories of firms outside the banking sector in the United States. The position in the United Kingdom was likewise extended with the inclusion of comparable businesses in the Money Laundering Regulations 2001 and will be further extended by additional Money Laundering Regulations which are due to come into force early in 2004.

[46] Including bankers, money services and other professionals defined by the Money Laundering Regulations.

Kingdom generally. This amendment has increased the use of the power.[47] **Three amendments would enhance its effectiveness and fairness.**

a. **Open hearings in an ordinary Magistrates' Court are not the appropriate forum for handling cash seizures in terrorist cases. Such hearings are relatively infrequent and often depend on sensitive intelligence that the police may not be able to convert into open evidence within the 48 hours currently permitted between the seizure and confirmation in court. The procedure for warrant hearings in arrests under the Terrorism Act makes special provision for these difficulties.[48] In our view, the Terrorism Act should be further amended to enable initial cash seizure hearings to be handled similarly, subject to later confirmation in open court under the normal rules of evidence.**

b. Counter-terrorist police report cases where they have been unable to seize non-cash items which give rise to equally strong suspicions of terrorism: including, for instance specialist communications equipment or precious stones which are readily convertible into cash. **Powers of seizure should be extended to non-cash items where the police can show that they will have a direct role in preparing for, or carrying out, acts of terrorism.**

c. **The provision that cash is to be held in an interest-bearing account[49] during the course of proceedings is designed to compensate the individual where a terrorist link proves unfounded. Alternative means of compensation in cash seizure cases for those Muslims with religious objections to profiting from interest should be devised.[50]**

Account Monitoring Orders

125. Schedule 4 extends the range of information that the police can request from banks in the course of a terrorist investigation. Account Monitoring Orders:

a. which previously could last for 28 days, can now be placed for 90 days;

b. can require information to be supplied immediately, rather than at the end of a given period.

Usage

126. The total number of account monitoring orders granted under Schedule 2, Part 1, is 8. They have not been used since April 2003.

[47] Compare the use of the preceding power between February and December 2001, under which only £18,500 was seized.

[48] The Terrorism Act 2000 deals with this under Schedule 8, paragraphs 29 and 34. Warrants for extended detention after 48 hours' initial arrest without warrant are subject to the decision of a Senior District Judge or his Deputy, or a specialist District Judge (Magistrates' Courts) specifically designated for this role by the Lord Chancellor. When the appropriate judicial authority permits, the decision may be made while the individual concerned and his representatives are not present, and only the general grounds for further detention need be revealed to them.

[49] Schedule 4, Part 2, 4 (1).

[50] Any such provision should be subject to thorough consultation with Muslims. We asked the Forum Against Islamophobia and Racism for their advice on how to address this problem; their view was that Muslims should obtain their compensation and donate it to charitable and humanitarian causes.

Our view

127. This provision created a power of significantly extended scope. We note that very limited use has been made of the orders. At present, banks are not able to process many types of information sufficiently quickly to meet the requirements of the orders, which raises questions about their utility.

128. In our view, **the Government should report to Parliament during the debate on this Committee's report on whether it is likely that there will be any further use of the Schedule 2 account monitoring orders – and, if it is proposed to retain the power, on the action that they propose to take to give them a realistic practical foundation. We draw this matter to the attention of the Treasury and Home Affairs Select Committees.**

Requirement to report

129. The Terrorism Act 2000 makes it an offence for a person who, by virtue of information that has come to him in the course of a trade, profession, business or employment, believes or suspects that another person has committed an offence under Sections 15-18 of the Terrorism Act (i.e., terrorist fund raising and money laundering) not to notify the authorities. Schedule 2 of the 2001 Act makes it an offence for members of the regulated sector[51] to fail to report where they "know or suspect, or have reasonable grounds for knowing or suspecting" that such an offence has been committed. This creates an objective test for criminal liability: individuals are liable to prosecution where such grounds exist, regardless of whether they had such a suspicion in fact.

Usage

130. There have been no prosecutions for failure to report a suspicious transaction under Schedule 2, Part 3.

Our view

131. As Lord Carlile notes, "There are concerns in businesses in the regulated sector about difficulties of compliance, and the serious consequences that may flow from errors of judgement or even failures to notice."[52]

132. We believe that the new objective test is a sounder basis for the prosecution of professionals in cases of complicity, or clear failure to co-operate with the authorities, but the development of strong joint working methods between the industry and the police is the most effective way to detect patterns of terrorist finance. This demands particular vigilance from the industry in keeping pace with emerging funding patterns: for financial crime specialists in the banks, this has meant developing the capacity to track multi-dimensional networks of transactions which, in themselves, may be entirely legitimate and unsuspicious. This level of vigilance goes beyond the usual requirements in relation to "ordinary" financial crime.

133. In this context, a punitive approach alone is inappropriate; it is vital for the authorities to work closely with the industry to ensure that the information that they obtain is of maximum value in detecting and countering terrorism. The police together with regulators and professional organisations have taken steps to raise awareness and enhance information-sharing with the regulated sector, including seminars, and issuing

[51] See footnote 46 on page 36.
[52] *Report on the Operation in 2001 of the Terrorism Act 2000,* pages 19-20.

terrorist finance guidance notes. In the interests of improving their own terrorist reporting, the industry would still like to see a clearer lead from the authorities in sharing intelligence on emerging patterns, and better feedback on the criteria which the authorities apply in fast-tracking particular reports of suspicious activity for further work. **Some mechanism for sharing more specific information on terrorist finance and reporting requirements should be developed between the law enforcement authorities and the financial services industry. We draw this to the attention of the Treasury and Home Affairs Select Committees.**[53]

Suspicious Activity Report regime

134. The Part 1 requirement on the financial sector to report activities giving rise to suspicion (in the form of "Suspicious Activity Reports", usually abbreviated as "SARs") is similar to provisions in the Proceeds of Crime Act 2002 (POCA), which impose an obligation on regulated financial services to report suspicious activity relating to money laundering.[54] In the first year of the new POCA regime, a very large number of reports were filed, of which only a small number derived from specifically terrorist suspicions. A recent report[55] looked at the considerable practical difficulties which have been presented by the scale of reporting under this new requirement and made recommendations, which have been accepted, for better reporting and more efficient processing of the reports once filed. It is important that the prevention of terrorism, where speed of response is crucial, should remain a high priority under the new system.

135. We note that there is currently no requirement that the police should destroy SARs in cases where the account-holder turns out to be innocent. As noted above, the scale of reporting became very large following the Proceeds of Crime Act, and the grounds for making such reports are not always well-founded.[56] There is a risk, therefore, that extensive financial information will be collected regarding completely innocent individuals.

136. The legislation requiring the regulated sector of the financial industry to submit such reports regarding their clients' activities should be amended to protect the privacy of innocent individuals and bodies corporate, by requiring the authorities to destroy reports in cases where charges are not brought or are disproved. An exception should be made only where appropriate authorisation is given that the report in question is material to an ongoing terrorist investigation.

Other remarks

137. Investigations into terrorism have highlighted a number of weak points in international regulation from which terrorists might potentially benefit; in the light of these, a

[53] Representatives of the industry suggested that specialists in the banks' financial crime units might undergo a developed vetting (DV) process as a basis for such a development.
[54] Proceeds of Crime Act 2001 Section 330.
[55] *Review of the regime for handling Suspicious Activity Reports*, (KPMG) published July 2003. Between 1995 and 2000 there were 15,000 such reports per year on average. The figure rose sharply to 63,000 in 2002, and the Report predicted some 100,000 reports would be submitted by the end of 2003. Recent reports suggest that the figure may rise still further to 150,000 in 2004, once forthcoming Money Laundering Regulations have brought more categories of business within the Suspicious Activity reporting regime: Financial Times, 28th November 2003. The same report noted the observation by Angela Knight (Chief Executive of Private Client Investment Management) that when confronted by reporting on this scale, the police were unlikely to follow up any such reports unless they already had information on the individual concerned.
[56] For instance, the KPMG report quoted the stated grounds for one report: "I didn't like his attitude", page 33.

specialist international organisation addressing money laundering, the Financial Action Task Force (FATF), issued 8 special recommendations on terrorist finance on 31 October 2001.

138. The unregulated character of some remittance systems, including hawala,[57] was a matter of concern. We are pleased to note that providers of such services are now required by the Money Laundering Regulations 2001 to register as a money service business and are therefore subject to ordinary financial business regulations.

139. Anonymous wire transfers, which historically have been susceptible to abuse by terrorists, were the subject of a special recommendation: they played a notable part in the funding of the 11 September attacks.[58] Money Laundering Regulations now in draft would require wire transfers by cash transmitters to be accompanied with sufficient originator information to permit the identification of the individuals involved. The delay in laying the relevant regulations before Parliament [59] is regrettable, but we are told that they will come into force early in 2004. Once they are in place, the United Kingdom will fulfil all the FATF special recommendations.

[57] "Hawala" is one of a number of alternative or parallel remittance systems operating outside traditional banking or financial channels. Similar systems were developed in a number of countries before the introduction of western banking practices. The components of hawala that distinguish it from other remittance systems are personal trust and the extensive use of connections such as family relationships or regional affiliations.

[58] Significant sums were transferred from abroad into US accounts in this way. Participants in the attacks subsequently withdrew the money in small quantities through ATMs to avoid suspicion.

[59] The intention had been to present them to Parliament before the Summer Recess in 2003.

D.2: Part 2 – Freezing Orders

Provisions

140. Part 2 repealed and replaced legislation[60] that provided for the freezing of the UK assets of foreign governments and certain foreign individuals in times of serious emergency. These had their origin in measures passed early in the Second World War.

141. Previously the powers could be used only where action to the detriment of the UK economy had been taken or was likely. In practice this meant the outbreak of armed hostilities. Part 2 also allows asset freezing in cases where action constituting a threat to the life or property of UK nationals has been taken or is likely. In principle, such action might include:

    a. a terrorist threat,

    b. actions by governments which fall short of war but which nevertheless constitute a threat against specific UK nationals or property.

142. Financial sanctions of this sort have more impact where they can be implemented internationally on the basis of multilateral agreement.[61] Analogous legislation for asset freezing is in place providing for the implementation of freezing orders on the basis of United Nations or European Union agreement. Part 2 is geared to those other occasions where action has not yet been agreed internationally, or where it is appropriate for the United Kingdom to impose sanctions unilaterally.

Usage

143. This part of the Act remains unused.

Our view

144. The circumstances in which assets might be frozen are broad. There is no mechanism in the legislation for appeal or independent review of any such order once approved. The Government has argued[62] that:

    a. international commercial agreements would act as a check on their use outside genuine emergencies;

    b. the requirement for affirmative resolution of any such orders would also guard against unjustified use;

    c. the orders lapse two years after their introduction;

    d. the orders would be subject to ordinary judicial review;

---

[60] Emergency Laws (Re-enactments and Repeals) Act 1964 Section 2.
[61] The UN Committee charged with the oversight of sanctions against al Qaeda recently highlighted poor implementation of freezing orders in many countries as an obstacle to effective action: www.un.org/Docs/sc/committees/1267Template.htm.
[62] House of Lords Debates: 28th November 2001, cols. 353-4.

e. finally, the Treasury has a duty to:

i. keep the orders under continuing review;

ii. give reasons in writing for any such order on request.

145. These safeguards may be adequate for truly emergency powers to be exercised in time of war, but their adequacy remains untested outside those very particular circumstances.

Other freezing orders for use against terrorists

146. These measures are unlikely to be used against terrorism while the Terrorism (United Nations Measures) Order 2001 is in place, which already makes specific provision for freezing terrorist assets.

147. The order implements United Nations Security Council Resolution 1373, as passed by the Security Council on 28 September 2001,[63] which required states to implement a co-ordinated freezing of terrorist funds internationally. Another instrument, *Al Qa'ida and Taliban (United Nations Measures) Order 2002* implemented the separate requirements of UNSCR 1390. A large number of orders freezing the assets of al Qaeda and other terrorist groups and individuals have been imposed in this way by the Treasury since 2001.[64]

148. From the counter-terrorist point of view, the Terrorism Order has a number of advantages which distinguish it from Part 2:

a. it gives a clear and narrowly limited definition of terrorism, drawn directly from the Terrorism Act 2000;[65]

b. it is not limited in application to foreign nationals (and thus for instance has been used against the assets of the UK suicide bombers);

c. it explicitly permits an appeal by individuals and affected firms through the High Court, unlike Part 2 where the only provision for scrutiny after an order is made is by a process of internal review of an unspecified character by the Treasury.

149. The provisions of Part 2 are intended for much wider use. In our view, **freezing orders for specific use against terrorism should be addressed again in primary terrorism legislation, based on the well-tested provisions of the Terrorism (United Nations Measures) Order 2001.**

150. **Freezing orders for other emergency circumstances, and the safeguards which should accompany them, should be reconsidered on their own merits in the context of more appropriate legislation for emergencies; the present Part 2 powers should then lapse. The forthcoming Civil Contingencies Bill would seem to be a suitable opportunity.**

[63] The order was made under powers created by Section 1 of the United Nations Act 1946.
[64] A list of the existing orders under these and other powers is maintained on the Bank of England website; see: www.bankofengland.co.uk.
[65] As defined in Section 2 of the Order.

D.3: Part 3 – Disclosure of Information

Background

151. In June 2000 the Performance and Innovation Unit's (PIU's) report *Recovering the Proceeds of Crime* recommended that

> *Legislation should be introduced to allow the Inland Revenue to disclose information on a case by case basis for the purpose of determining whether to initiate, pursue or bring to an end criminal investigations or proceedings. Consideration should be given to whether this legislation should extend to all public bodies and also to assisting foreign criminal investigations or proceedings.*

152. This proposal was included in Part 2 of the Criminal Justice and Police Bill in January 2001. The provisions were, however, dropped from that Bill, in the face of opposition in the House of Lords, to allow the passage of the remainder of the Bill before the 2001 general election. They were taken up again and enacted in Part 3 of the Anti-terrorism, Crime and Security Act 2001.

Provisions

153. Part 3 allows public bodies to disclose information to assist criminal investigations or proceedings, whether in the UK or abroad, including whether investigations or proceedings should be initiated or brought to an end. In addition, it allows the Inland Revenue and HM Customs and Excise to disclose information to the intelligence and security agencies (the Security Service ("MI5"), the Secret Intelligence Service ("MI6") and the Government Communications Headquarters (GCHQ)).

154. The public bodies to which Part 3 applies are defined implicitly by their (pre-existing) information disclosure powers – 66 such powers are listed in Schedule 4. These allow the disclosure of information obtained during the course of investigations into efficiency, compliance with regulatory regimes,[66] and information obtained from farmers and fishermen,[67] for example. The Treasury may, by order, add any provision contained in subordinate legislation to the Schedule 4 list. No such order has yet been made.

155. It follows that information obtained by public authorities under statutory powers conferred for one purpose may be disclosed to the police and intelligence and security agencies to be used for completely different legitimate purposes (e.g., for any criminal investigation which "may be carried out"). The Data Protection Act 1998 and the Human Rights Act 1998 continue to apply. These provide some additional protection against disclosure. The Secretary of State may prevent the disclosure of information under this Act to overseas jurisdictions that do not offer an "adequate" level of

[66] For example by trading standards officers, employment agencies, the Office of Fair Trading, the Health and Safety Executive, the Equal Opportunities Commission, and Commission for Racial Equality.
[67] For example by agricultural marketing boards, the Meat and Livestock Commission, Home Grown Cereals Authority, and Sea Fish Industry Authority.

protection, in circumstances where it would be more appropriate for the investigation to be carried out by the UK authorities or those of a third country.[68]

156. In practice, the requirement that the recipients of confidential information need to be capable of carrying out criminal investigations or prosecutions means that the majority of disclosures within the UK are likely to be made to the police, the National Criminal Intelligence Service (NCIS) and the National Crime Squad, although a range of bodies with more specialised investigatory functions, such as Her Majesty's Customs and Excise, the Scottish Drugs Enforcement Agency, the Financial Services Authority, Serious Fraud Office, Office of Fair Trading, Department of Trade and Industry, Immigration Service, and Health and Safety Executive may also be potential recipients.

Usage

157. The Inland Revenue (which has, in our view, implemented the disclosure regime in a responsible way) has provided us with the following data about the number of disclosures that they have made to the police and intelligence services under Section 19. The figures include a large number of disclosures relating to Operation Ore.[69] Excluding that operation would reduce the proportion of information disclosures relating to sex offences to under 20%.

Table 1 Disclosures by Inland Revenue (January 2002 - September 2003)

Murder	*Sex Offences*	*Drug Offences*	*Terrorism*	*Financial Offences*	*Violent Crime*	*Others*	*Total*
821	9,157	4,848	701	3,390	372	620	19,909
4%	46%	24%	4%	17%	2%	3%	100%

158. HM Customs and Excise made 796 disclosures up to September 2003. Of these, 169 (21%) were related to terrorism. Disclosures by other public bodies have not been systematically monitored. We believe that they should be.

159. We understand that no use has yet been made of the facility to disclose to overseas jurisdictions (which would create the potential for overseas authorities to get information from UK public bodies that in most countries they could not get from their domestic ones).

Our view

160. During the passage of the Bill Parliament was given the impression by Government that the Part 3 powers to disclose confidential information did not represent a substantial change,[70] presumably on the grounds that information was already being disclosed in

[68] See House of Commons Library Research Paper 02/54, *The Anti-terrorism, Crime and Security Act 2001: Disclosure of Information*, by Edward Wood, 4th October 2002, for a fuller account.

[69] Operation Ore is a national police enquiry into the involvement of United Kingdom residents in certain American websites that supplied indecent photographs of children. Investigations were prioritised according to the occupation of the suspect using information held by the Inland Revenue. Some prosecutions have already received national media attention.

[70] For example, House of Commons Debates: 26 November 2001, cols 793-4:

certain limited circumstances. Before Part 3 was enacted, the disclosure of information by public bodies was limited, for the most part, to the exercise of their functions, except in some marginal and legally uncertain cases. It has been argued that in common law the duty to the public might override the duty of confidence owed by a public authority with regard to a particular item of information in some cases (for instance where the information concerns the commission of a criminal offence or relates to life-threatening circumstances).[71] For example:

a. historically the Inland Revenue disclosed information in murder or treason cases (even after they ceased to attract the death penalty);[72] and

b. HM Customs and Excise provided information to the police and other law enforcement agencies on a case-by-case basis where there was an over-riding public interest justification for doing so.

161. However, despite these instances of past practice and ministerial assertions to the contrary, these provisions are, in our view, a significant extension of the Government's power to use information obtained for one purpose, in some cases under compulsory powers, for a completely different purpose.

162. Part 3 clearly falls into the category of mainstream legislation applicable to the investigation and prosecution of crime in general.

163. We attach particular importance to the principles set out in Article 8 of the Human Rights Act:

> *Right to respect for private and family life*
>
> *Everyone has the right to respect for his private and family life, his home and his correspondence.*

"The Economic Secretary to the Treasury (Ruth Kelly): The hon. Member for Beaconsfield (Mr. Grieve) fundamentally misunderstands the nature of these clauses. Clause 17 is designed to clarify for public officials in what circumstances they may disclose information. I think that many Members will recognise the need for that clarification. If the clause were restricted to terrorist offences, it would be a significant impediment because the public official in each case would have to satisfy himself in advance of any disclosure whether the information was directly related to a terrorism investigation. That does nothing to harmonise requirements or to make it simple for public officials to understand what they are supposed to disclose.

Mr. Grieve: We do not want to make it simple. I am sure that the Minister will agree that each of the sections of each of the Acts listed in schedule 4 contain specific protections. She can read them. I quoted section 28(7) of the Health and Safety at Work, etc. Act 1974. Protection exists, but she intends to get rid of it. That is hardly a clarification.

Ruth Kelly: I thank the hon. Gentleman for his intervention, but it again shows that he fundamentally misunderstands the nature of the clause.

The hon. Gentleman disputes the fact that the clause contains safeguards. I guarantee that it provides strong safeguards for the disclosure of information. I emphasise that all the gateways in clause 17 are pre-existing: they have already been approved by the House, and nothing new is being debated today. They refer to specific information covered by existing statutory restrictions on disclosure. Safeguards are provided by the Human Rights Act 1998 and by the Data Protection Act 1984, and they still apply, so any information that is disclosed must be proportionate, necessary and lawful."

[71] *Privacy and Data-Sharing: the Way Forward for Public Services*, PIU, April 2002, Annex A, page 15.

[72] For details, see *Royal Commission on Standards in Public Life*, Cmnd 6524, 1976, paragraph 93ff.

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

164. The protection offered by the Human Rights Act 1998 and the Data Protection Act 1998 seems to us to be illusory since the burden will lie on the individual to complain about the disclosure of their confidential information in circumstances where, almost by definition, he or she will be unlikely to know that disclosure has occurred.

165. We also endorse the conclusions reached by the Joint Committee on Human Rights,[73] that

> *"there remains a significant risk that disclosures will violate the right to respect for private life under Article 8 of the ECHR, because of the range of offences covered, and the lack of statutory criteria to guide decisions and the lack of procedural safeguards to be followed when deciding whether it is necessary and proportionate to make a disclosure of personal information."*

External oversight

166. **In our view the Government should legislate to provide independent external oversight of the whole disclosure regime (e.g., by the Information or one of the other statutory Commissioners) to provide a safeguard against abuse and to ensure that rigorous procedural standards governing disclosure are applied across the range of public bodies, prosecuting authorities and intelligence and security agencies. It should also require the independent overseer to publish statistics twice a year on the use of Part 3 (both within the United Kingdom, and to overseas authorities).**

Authorisation

167. External oversight is a necessary safeguard, but it is not, in our view, sufficient.

168. In the past, where a statute conferred intrusive powers on the executive, Parliament has normally made their exercise subject to the prior approval of a judge or other independent person (e.g., search warrants). Independent authorisation or scrutiny has been considered particularly important when an individual is unlikely to know that such powers are being exercised against him, as is the case here.

169. The rigorousness of such a prior authorisation safeguard should be a function of two factors:

    a. the seriousness of the crime being investigated or prosecuted (in terms of the sentence that it would attract, for example); and

    b. the sensitivity of the information being disclosed.

[73] Joint Committee on Human Rights, *Anti-terrorism, Crime and Security Bill: Further Report*, HL 51/HC 420, paragraph 24, http://www.publications.parliament.uk/pa/jt/jtrights.htm.

170. **In our view, internal authorisation by a senior person would be adequate for the disclosure of addresses or phone numbers in terrorism cases.**

171. **While we accept that it may well be that the same regime could be justified for other types of serious crime, we would argue that prior judicial approval should be required in any case involving less serious crimes or the disclosure of more sensitive information. Parliament should be given the opportunity to decide what level of authorisation should be required, depending on the seriousness of the crime and the sensitivity of the information being disclosed.**

D.4: Part 4 – Immigration and Asylum

Background

172. A primary objective for the authorities is to prevent terrorism before it occurs. They have a range of potential options for dealing with suspected terrorists which include surveillance, prosecution, disruption, and in the case of foreign suspects, deportation or extradition.

173. Part 4 adds to these options by allowing the potentially indefinite detention of certain foreign terrorist suspects.

Provisions

174. Part 4 has required derogation from the right to liberty under the European Convention on Human Rights. It allows the Home Secretary to certify foreign nationals whom he reasonably suspects of having links with groups linked to Osama Bin Laden and al Qaeda[74] as "suspected international terrorists"[75] and detain them,[76] subject to bail, if they cannot be deported either because of the UK's international obligations (e.g., they would face inhuman or degrading treatment)[77] or for practical reasons. A suspect may choose to leave the UK if he can find a state prepared to take him.

175. Suspects are neither charged nor prosecuted. Instead the Home Secretary certifies that he reasonably

    a. believes that their presence in the UK is a risk to national security; and

    b. suspects that they are international[78] terrorists.

176. They can then be detained in high security conditions. They may appeal against certification to the Special Immigration Appeals Commission (SIAC)[79] which is presided

[74] The limitation to people linked to al Qaeda and associated groups is not set out explicitly in the legislation. It follows from the derogation from the ECHR which was based upon the threat from al Qaeda. In July 2002 the Special Immigration Appeals Commission found that "In the present situation there are two reasons for supposing that the provisions of sections 21 to 23 of the 2001 Act are to be applied only to those said to be linked to al Qaeda and its associates. First, the 2001 Act falls to be interpreted in the light of section 3 of the Human Rights Act, which would tend to prevent the powers of detention being exercised in the absence of a connection with the state of emergency. Secondly, the Attorney-General indicated to us on behalf of the government that if the powers under sections 21 to 23 of the 2001 Act were exercised against a person not said to be linked with al-Qaeda or its associates, that would be a proper basis for this Commission to set aside the certificate under section 25(2)(b) of the Act." (SIAC Appeal No: SC1 1-7/2002, paragraph 48). The Court of Appeal also endorsed the limitation unanimously in October 2002. A fuller discussion of the scope of Part 4 can be found in the Special Immigration Appeals Commission's generic judgement of 29th October 2003 on Appeals SC/1,6,7,9,10/2002, paragraphs 85ff.

[75] Anti-terrorism, Crime and Security Act 2001 Section 21.

[76] Anti-terrorism, Crime and Security Act 2001 Section 23.

[77] Contrary to Article 3 of the European Convention on Human Rights.

[78] That is, they are subject to the control or influence of people outside the UK.

over by a high court judge, sitting without jury. The appeal process considers whether or not there are reasonable grounds for the Home Secretary's belief or suspicion.[80] It comprises two elements:

a. an "open" element involving material that the Home Secretary is prepared to disclose; and

b. a "closed" element involving material that he is not prepared to make public.[81] In this element the interests of the suspect are represented by a security-cleared "special advocate". Once the special advocate has received the closed material, he may no longer communicate with the suspect or his legal representatives (although he may continue to receive material from them).[82]

177. In practice, people certified as suspected international terrorists under Part 4 powers may be detained under other powers (e.g., if they are subsequently convicted of an offence).

178. There is no explicit detention period. Detention under Part 4 ceases if

a. an acceptable country can be found to take the suspect, and he is willing to leave the UK;

b. the Special Immigration Appeals Commission grants bail or finds that there are no reasonable grounds for the Home Secretary's belief or suspicion;

c. the Home Secretary revokes the certificate; or

d. the detention powers lapse.[83]

---

[79] The Special Immigration Appeals Commission was initially created by the *Special Immigration Appeals Commission Act 1998*, following a decision by the European Court of Human Rights (Chahal v. UK (1996) 23 EHRR) criticising the lack of an appeal to an independent tribunal in UK law if an immigration decision (such as refusal of leave to remain, or the decision to deport an individual) was based on national security or political grounds. The existing advisory panel – the "three wise men" – was judged not to be sufficiently independent to constitute a court under Article 5 of the European Convention on Human Rights, in that the appellant was only given an outline of the grounds for the notice of intention to deport, the panel had no power of decision and its advice to the Home Secretary was not binding and was not disclosed. The 1998 Act provided a right of appeal to the Commission against almost all immigration decisions made on such grounds.
The following extract from the time of the 1991 Gulf War (House of Commons Debates: 7 February 1991, col. 405) illustrates the operation of the "three wise men" approach:

Mr. Kenneth Baker [Home Secretary]: One hundred and sixty two Iraqi citizens have been served with notices of intention to deport them on the grounds of national security since 2 August 1990. Of these, three have been deported and 77 have left the United Kingdom voluntarily.
…
The procedure is that I issue a notice of intention to deport. The person subject to that intention has a right of appeal to the advisory panel of three. If, as a result, I confirm the intention to deport, I issue a proper deportation notice. The person concerned also has a right of appeal in respect of the destination. We are currently discussing with some people the countries to which they wish to go…

[80] Anti-terrorism, Crime and Security Act 2001, Section 25.

[81] The Special Immigration Appeals Commission (Procedure) Rules 2003, Rule 38 is intended to allow the special advocate to argue on the suspect's behalf for parts of the "closed" material to be made "open".

[82] The Special Immigration Appeals Commission (Procedure) Rules 2003, Rule 36.

[83] The Part 4 certification and detention powers (Sections 21-3) lapse on 10th November 2006. Before then, their continuation is subject to periodic Parliamentary approval. The current continuation Order lasts until March 2004.

Usage

Policy

179. The Government has said that certification and detention under Part 4 is a last resort, where neither prosecution nor removal from the country is possible. In seeking to bring prosecutions, the authorities face a range of issues relating mainly to whether the material that forms that basis of their case would be admissible as evidence in court,[84] and, if it is, whether they would be prepared to disclose it. In particular, there is a statutory prohibition on the use of intercepted communications as evidence in court. The authorities may have good reasons for not wanting to expose intelligence to the suspect (e.g., to protect sources and techniques or to avoid damaging relations with foreign governments or agencies).

180. The House of Lords was told during the passage of the Bill that it was for the Crown Prosecution Service to judge whether there was sufficient evidence to prosecute.[85] The police, in conjunction with the Security Service, consider the scope for action against a foreign national (including referring a case to the Crown Prosecution Service) where intelligence suggests involvement in international terrorism.

181. In deciding whether to use the Part 4 powers, the authorities have regard not only to the likelihood of securing a conviction, but also the extent to which the likely sentence would address the potential threat posed by the suspect (a factor in the decision to use

[84] Evidence can be inadmissible in ordinary trials because of the risk of an improper conviction, either because its weight or credibility cannot be effectively tested, or because it has prejudicial rather than probative value and so may be misinterpreted or misused by a jury, for example. See paragraph 228ff for some further discussion of these issues.

[85] House of Lords Debates: 29 November 2001, col. 509:
Lord Rooker: … We have made it clear on a number of occasions that detention under Part 4 will only be used for a limited number of people, where no other response is possible. If we consider that there is sufficient admissible evidence to bring a prosecution, we will seek to do so at any point in the process. If we can prosecute, we will. That is our first priority. Our second priority is to remove the individual. It may be that one process is used, then evidence becomes available. One has to assume that we would take action on those lines.
…
Lord Rooker: …
We shall prosecute if there is admissible evidence. We shall do all we can to find a way of removing someone from the country, including an assessment of possible safe third countries. We shall, of course, abide by our international obligations, as the Attorney-General has made clear. I hope that there is no doubt about the Government's sincerity.
A separate question is whether it should be stated as a requirement of the Bill that the Secretary of State will not detain someone under Clause 23 unless, for example, he has done all that he reasonably can to bring about a criminal prosecution. That sounds seductive but if there is to be such a test, the implication is that SIAC will review the Secretary of State's compliance with that test…
We strongly argue that the question of whether or not a criminal prosecution is to be brought is not for SIAC or within its competence but is for the prosecuting authorities…
I do not see SIAC or any other court as an appropriate body for making judgments about the sufficiency of evidence upon which to bring a prosecution. That matter is for the Crown Prosecution Service. It will already have reached the view that there is insufficient evidence and that it is not in the public interest to prosecute.
Independent discretion is an issue of constitutional importance and is covered by the guidelines applying to the Crown Prosecution Service. Such discretion is totally inappropriate for a body such as SIAC, which has no expertise in the criminal field. The implications of a body such as SIAC deciding that there is sufficient evidence to bring a prosecution, notwithstanding the objection of the police and CPS, would taint the individual with a "guilty" label before he or she even got to court.

Part 4 that has not been emphasised).[86] For example, if the successful conviction of a terrorist suspect for credit card fraud was likely to lead to detention for a matter of months, the authorities might still pursue certification and detention under Part 4. We would anticipate that the Special Immigration Appeals Commission would comment, if not allow an appeal against certification and detention, if it considered that prosecution for a sufficiently serious crime seemed possible in a particular case.

182. Where successful prosecution is not thought likely, or the potential sentence is thought to be insufficient but the person concerned is considered to be a threat to national security, the Security Service may recommend that the person be deported from the UK, on the basis that his presence here is not conducive to the public good for reasons of national security. Where appropriate, the Security Service will also recommend that if the person concerned cannot be deported, because of ECHR considerations or because of practical difficulties, they should be certified and detained under the Part 4 provisions of the Act. The decision as to whether to recommend certification to the Home Secretary is taken by the Home Office in consultation with the intelligence agencies, the police and Foreign and Commonwealth Office.

Statistics

183. The Home Secretary set out the facts on the use of Part 4 in a written statement on 18th November:[87]

> *Sixteen foreign nationals[88] have so far been detained using powers in Part 4 of the Anti-terrorism Crime and Security Act 2001. Eight were detained in December 2001, one in February 2002, two in April 2002, one in October 2002, one in November 2002, two in January 2002 and one in October 2003. One further individual has been certified under Part 4 of the Anti-terrorism, Crime and Security Act in August 2003 but is detained under other powers.*
>
> *Of the total detained, two have voluntarily left the United Kingdom [for France and for Morocco]. The other fourteen remain in detention…*

184. Ten appeals against certification were heard by the Special Immigration Appeals Commission in May to July 2003, up to eighteen months after most of those certified had been detained. It rejected them all on 29th October 2003. The cases are subject to a further level of appeal, but only on points of law. A further appeal against certification started on 19th November 2003 and more are scheduled to begin on 15th December and in the New Year.

---

[86] Special Immigration Appeals Commission generic judgement SC/1,6,7,9,10/2002 (29th October 2003): "25 … In summary, not all those who might fall within the scope of the 2001 Act and the derogation had been detained: it would depend on such matters as the strength of the intelligence case, the prospect and gravity of any criminal proceedings, possible length of sentence, the management of the risk whether defensively or to obtain information, the prospect of deportation, and the significance of the threat which they were assessed to pose and whether detention was proportionate to that threat. Resources for detention was relevant. It was unlikely, if the danger warranted detention, that compassionate or family circumstances would prevent it, said witness A, in closed session. Obviously the individual would have to be a foreign national who met the statutory tests."

[87] House of Commons Debates, 18th November 2003: col. 27WS.

[88] [The personal details of the detainees are protected, except where the names of the individuals concerned are in the public domain and they have no objection to being identified].

Our view

Problems presented by Part 4

185. The Part 4 detention powers present a number of problems that range from fundamental issues of principle to practical procedural difficulties. We are not persuaded that the powers are sufficient to meet the full extent of the threat from international terrorism. Nor are we persuaded that the risks of injustice are necessary or defensible.

186. Some of these problems arise because Part 4 is an adaptation of existing immigration and asylum legislation, rather than being designed expressly for the purpose of meeting the threat from international terrorism.

Problems of principle

187. *The suspects face no specific charge and are not presented with, and given the opportunity to refute, all the evidence against them.*[89] This is a significant limitation in what is an essentially adversarial legal process and increases the risk of a miscarriage of justice. This risk is compounded by the following features of the process:

a. *The standard of proof involved in the Special Immigration Appeals Commission procedure is low*. It is "reasonable belief and suspicion", and not even "a balance of probabilities", much less proof "beyond all reasonable doubt";

b. The current *Special Immigration Appeals Commission rules do not oblige the Home Secretary to reveal all material which could help the suspect* (even in summary form);[90]

c. In some cases the vast majority of the case is closed and so the *open case might be an unreliable indication of the basis of the closed case*.

188. *It has required the UK to derogate from the right to liberty under Article 5 of the European Convention on Human Rights.* Article 5 says:

> ***Article 5 – Right to liberty and security***
>
> *1. Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:*
>
> *(a) the lawful detention of a person after conviction by a competent court;*
>
> …

[89] One way in which this manifests itself has been set out by the Special Immigration Appeals Commission in the generic judgement of 29th October 2003 on appeals SC/1,6,7,9,10/2002: "117 … We are conscious that cross-examination of [a suspect] proceeds on a basis where he does not know the significance of some of the questions being asked or the extent to which they may seek to lay the groundwork for a contradiction with [material that he will not see and], with which he cannot deal except to the extent that he may have anticipated the point and provided other material to the special advocates to use as they saw fit."

[90] The generic judgement on Special Immigration Appeals Commission Appeals SC/1,6,7,9,10/2002 (29th October 2003) paragraphs 52-4 discusses this issue and explains that the Special Immigration Appeals Commission disclosure system leaves control over disclosure in the hands of one party and its fair operation depends on the integrity of the [Home Secretary's] team and its understanding of what might actually assist an appellant. SIAC also commented (paragraph 281 of the same judgement) that it did not think that there had been any unfair holding back of material, although they were not in a position to know for sure.

> *(f) the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition.*

Since the courts[91] have established that detention of a person where there is no realistic prospect of removal is not covered by "detention of a person against whom action is being taken with a view to deportation", Part 4 requires a derogation from the right to liberty.

189. *The UK is the only country to have found it necessary to derogate from the European Convention on Human Rights.* We found this puzzling, as it seems clear that other countries face considerable threats from terrorists within their borders.[92] Indeed, there have been a number of convictions and deportations[93] of terrorists and terrorist suspects in other European countries. It has sometimes been suggested that lawyers and courts in other countries are less rigorous than those in the UK or that other countries may have repatriated terrorist suspects without taking full account of human rights considerations. We have seen no evidence that other countries have disregarded their international obligations, but some countries have reached understandings on the treatment of their deportees with the destination countries.

190. Detention under Part 4 is for a *potentially indefinite period (see also paragraph 178)*.

191. It may be reassuring in some respects that these powers have been used on only 17 terrorist suspects. But there is another view, put eloquently by Justice Jackson of the US Supreme Court in 1948: "*nothing opens the door to arbitrary action so effectively as to allow … officials to pick and choose only a few to whom they will apply legislation and thus to escape the political retribution that might be visited upon them if larger numbers were affected*". [94]

Problems of efficacy

192. The Part 4 process *only tackles the threat from foreigners suspected of having links with al Qaeda or its associated networks.* It does not, therefore, address the threat:

    a. from British nationals with similar links; or from

    b. anyone in the UK with links to other foreign terrorist causes.

193. What is important is the nature of the threat, not the ideology behind it or the nationality of the perpetrator. The Home Office has argued that the threat from al Qaeda-related terrorism is predominantly from foreigners, but there is accumulating evidence that this

---

[91] *Chahal v United Kingdom* (1996) 23 EHRR.

[92] Broadcasts on Al-Jazeera attributed to Osama Bin Laden and Al Zawahiri, leader of the Egyptian Islamic Jihad and a close associate of Osama Bin Laden, have confirmed that Britain has been singled out as a target for al Qaeda. He said that the killing of the British and Australians in the Bali explosions were carried out by zealous sons of Islam. Britain, France, Italy, Canada, Germany and Australia were all threatened with killings and bombings for their part in joining with America in the invasion of Afghanistan. See page 30 for some specific examples.

[93] For example, on 18th November 2003 Abdel Qadir Fadlallah Mamour, an imam in Carmagnola near Turin, was deported to Senegal, his country of birth, "for disturbing public order and being a danger to state security". Six Moroccans and an Algerian were also deported. They were accused of proselytizing on behalf of "terrorist organizations with an Islamic origin." Several were trained in paramilitary camps and two of them have had contacts with militants taken prisoner by the U.S. Army in Afghanistan, according to news reports.

[94] *Railway Express Agency v New York* 336 US 106 (1949) at 112-113.

is not now the case. The British suicide bombers who attacked Tel Aviv in May 2003, Richard Reid ("the Shoe Bomber"), and recent arrests suggest that the threat from UK citizens is real.[95] Almost 30% of Terrorism Act 2000 suspects in the past year have been British.[96] We have been told that, of the people of interest to the authorities because of their suspected involvement in international terrorism, nearly half are British nationals.

194. There are also arguments of principle against having *discriminatory provisions*[97] with which we have a good deal of sympathy, but it is the arguments of limited efficacy in addressing the terrorist threat that weigh most heavily with us.

195. *Seeking to deport terrorist suspects does not seem to us to be a satisfactory response, given the risk of exporting terrorism.* If people in the UK are contributing to the terrorist effort here or abroad, they should be dealt with here. While deporting such people might free up British police, intelligence, security and prison service resources, it would not necessarily reduce the threat to British interests abroad, or make the world a safer place more generally. Indeed, there is a risk that the suspects might even return without the authorities being aware of it.[98]

196. We have heard evidence that the existence of these powers, and uncertainty about them, has led to understandable *disquiet among some parts of the Muslim population*. It is important that legislation against terrorism should attract wide public acceptance to maximise its effectiveness.

Problems of practice

197. *The process has been lengthy*, taking almost 1½ years between detention and the hearing of the appeal before the Special Immigration Appeals Commission, and almost 2 years before determination of the appeal. This is equivalent to a significant custodial sentence. Some of those involved argue that this is not intrinsic to the process and draw attention to earlier, pre-Part 4, Special Immigration Appeals Commission cases relating to attempted[99] deportations on national security grounds, which were less protracted. Others point to a range of factors which have contributed to the duration of the proceedings.[100]

---

[95] Other cases have involved a dual nationality Briton who was convicted on 27th September 2003 in Morocco in relation to the May bombings in Casablanca that killed 44 people (news reports 28th September 2003) and a British man from Birmingham who was arrested by the police in Pakistan on suspicion of links to al Qaeda, according to *The Times*, 31st October 2003.

[96] See Table 3: Results of Terrorism Act 2000 investigations (1st November 2002-4th November 2003), page 68, for further details. Not all of the 30% would be linked to networks linked to al Qaeda.

[97] See, for example, the Special Immigration Appeals Commission judgement of July 2002 which found that the derogation from the European Convention on Human Rights associated with Part 4 was incompatible with Articles 5 and 14 of the ECHR because it discriminated on the ground of nationality. (This was overturned by the Court of Appeal in October 2002 and is now before the House of Lords.)

[98] Special Immigration Appeals Commission SC/10/2002 (29th October 2003) has commented:
"24. There is one other matter which we should mention before we close. As Ajouaou says in his statement, he was in Morocco when Abu Doha was arrested. Mr Emmerson [Mr Ajouaou's counsel] in his submissions made reference to Ajouaou's frequent travel between Morocco and the United Kingdom, even in the months before he was arrested. Those facts must cast serious and probably fatal doubt on any claim by Ajouaou that it would be in breach of an international Convention to return him to Morocco. It appears clear, however, that the Secretary of State was not aware of Ajouaou's travels and indeed we do not know whether he made the journeys in his own name. We do not regard the fact that Ajouaou had been travelling as pertinent to the Secretary of State's apparent view (implied in the certificate and in the detention under it, read in conjunction with section 23) that Ajouaou could not properly be returned to Morocco."

[99] There have been no successful deportations on national security grounds since 1997.

[100] These included:

- the initial argument over the legality of Part 4 (to be considered by the House of Lords);

198. *Each appeal requires a fresh security cleared special advocate who has not been exposed to closed material (see paragraph* 176.b *above). The supply of such advocates is limited.* It does not seem to be desirable to rely on a system for tackling terrorism that is limited in this way. It has been suggested to us that prohibiting the special advocates from communicating with suspects could allow them to be used again.[101] This would allow special advocates to increase their expertise and might help to address some of the delays in the process, but we are not persuaded that these advantages would outweigh the possible risks of injustice if a suspect was unable to brief his special advocate directly at the start of an appeal.

Application

199. Our difficulty, therefore, is primarily with the adequacy and acceptability of the Part 4 powers themselves rather than the way in which the powers have been operated in particular cases so far. Just as we have avoided trying to second guess the courts on the legality of the Part 4 powers, we have not sought to take a considered view on the way in which they have been operated in particular cases, which is more a matter for Lord Carlile of Berriew. That said, we have no reason to doubt that the Home Secretary has applied his judgement conscientiously. We would also like to acknowledge that the Home Office and prison service have provided accommodation for the Part 4 detainees that better reflects their unconvicted status, as the Home Secretary promised in response to a recommendation by Lord Carlile.[102] The detainees have chosen not to occupy it.

200. Given the novel and contentious nature of these powers we believe that there should be a continuous proactive effort to manage the individual cases of the suspects with a view to finding alternative ways of dealing with them (such as finding evidence that would support a prosecution). We were, therefore, surprised to learn that the authorities appear to have given no thought to what change in circumstances might lead them to conclude that an individual should be released or dealt with differently (beyond the general observation that detention under the Part 4 powers would cease if those powers lapsed or if new information came to light which put a different complexion on his case). We have

---

- the initial denial of legal aid for this type of appeal. (This has, apparently, also been an issue in the appeal to the House of Lords against the derogation from the European Convention on Human Rights);
- the failures by the parties (including the Home Office) to meet deadlines set by the Special Immigration Appeals Commission;
- the difficulty in finding dates suitable for all the legal representatives (who are well-regarded in their field and so tend to be in demand);
- the need for detailed arguments between the special advocate and the Government's lawyers over whether more of the closed material could be disclosed without harm. These arguments can be protracted. Although the right to challenge the non-disclosure of material to the appellant is clearly an essential safeguard in the context of the current process, it is open to question whether such additional disclosures as have been secured have had any material effect on the outcome of any appeal, given the low standards of proof involved (reasonable suspicion);
- the volume of material involved. It has been suggested to us that more helpful organisation of the closed material made available to the special advocates and prior training in its nature would be desirable.

[101] Although they would, of course, be allowed to *receive* material from the suspect and his "open" legal representatives.

[102] House of Commons Debates: 3rd March 2003, col. 588: David Blunkett: **"**… Lord Carlile … recommended that there might be a discrete and specific change to the way in which those held under Part 4 were held. I have authorised that we should make such a provision available should the individuals choose to take it up. It would not be appropriate compulsorily to move all 13 into one area against their will and I do not intend to get into a secondary dispute about that. Lord Carlile put perfectly valid arguments concerning the length of time for which they had been held and might be held, suggesting that we should consider that urgently, and I have agreed that we should."

been told that prior to the forthcoming post-appeal reviews,[103] to be heard by the Special Immigration Appeals Commission starting on 29th April 2004, the authorities will be considering any relevant new evidence including whether there have been any changes in circumstances that would mean that an individual no longer posed a threat. **From the evidence we have received, we are concerned that there has not been a sufficiently proactive, focussed, case management approach to determining whether any particular suspected international terrorist should continue to be detained under Part 4. Nor did it appear that alternative ways of dealing with them were under active consideration. This gap should be filled in time for the first sequence of post-appeal reviews.**

201. The documentation associated with the detainees and the management of their cases ought to be exemplary, given their unique status and relatively small number. Unfortunately, it has not always been. This is not just a matter of bureaucratic perfectionism. There have been consequences. For example, there has been at least one case where misunderstandings over a change in detention status made it difficult for legal advisors to gain access to a detainee. (Such errors are different from the administrative errors referred to in footnote 16, page 25,which relate to the substance, rather than the handling, of detention cases.) We are, however, assured that action is being taken to address these concerns which we have drawn to the attention of Lord Carlile and of the Home Office.

Legality

202. The legality of Part 4 and the accompanying derogation from the European Convention on Human Rights is being contested through the courts (on the grounds of proportionality and discrimination against foreign nationals).[104] We have avoided trying to form judgements on the legal validity of the provisions, which is a matter for the courts, but have considered Part 4 as it stands.

Replacing Part 4 as soon as possible

203. We consider the shortcomings described above to be sufficiently serious to **strongly recommend that the Part 4 powers which allow foreign nationals to be detained potentially indefinitely should be replaced as a matter of urgency. New legislation should:**

    a. **deal with all terrorism, whatever its origin or the nationality of its suspected perpetrators; and**

    b. **not require a derogation from the European Convention on Human Rights.**

204. **We set out below several alternative approaches that, in our view, whether alone or in combination, merit further development by the Government as possible bases for a more acceptable and sustainable approach, while the threat remains. There may be others.**

Prosecution

205. **We strongly support the Government's stated objective of prosecuting terrorists using the normal criminal justice system as the preferred approach.**

[103] Anti-terrorism, Crime and Security Act 2001 Section 26.
[104] See footnote 97 on page 54.

206. In January 2002 two Algerians were charged with membership of al Qaeda, but the charge was dropped before trial. In April 2003 they were jailed for 11 years after being found guilty of raising cash for terrorism, making them the first people with suspected al Qaeda links to be imprisoned in Britain.[105] This case illustrates the fact that, despite the difficulties, it is possible to prosecute at least some terrorist suspects in a conventional British court.

207. The existing range of terrorism-related offences is broad. It has not been represented to us that it has been impossible to prosecute a terrorist suspect because of a lack of available offences. The inhibiting factor in the cases to which the Part 4 procedure is applied seems to be that intelligence on which suspicion of involvement in international terrorism is based

    a. would be inadmissible as evidence in court; or

    b. the authorities would not be prepared to make it available in open court, for fear of compromising their sources or methods.

Relaxing the blanket ban on the use of intercepted communications in court

208. In our view, **one way of making it possible to prosecute in more cases would be to remove the UK's self-imposed blanket ban on the use of intercepted communications in court**. This was also the view reached by Lord Lloyd in his 1996 Report, to which we have seen no convincing response, and by Lord Carlile when giving evidence to the Home Affairs Select Committee on his review of the operation of Part 4.[106]

209. The Government did not accept the case for removing the ban on the use of intercepted communications as evidence when the Regulation of Investigatory Powers Act 2000 replaced the Interception of Communications Act 1985. The reasons given were, essentially, that allowing the use of intercepted communications as evidence would reveal the authorities' capabilities, prompting criminals to take more effective evasive action.[107] More recently the Home Secretary has said that the issue is under review,[108] and we understand that the review is likely to continue into the New Year.

---

[105] "Sentencing the men, Mr Justice Curtis said: 'You have not directly taken life or seriously injured anyone. But the terrorists, in order to carry out their terrible killings and maimings, need money, false papers and military-style materials. You both provided terrorists with the vital support and ran a well-organised and secretive cell.' The two men, who were living in Leicester and worked together in a factory in Corby, used numerous false identities between them. They were secretly part of an intricate network of terror cells across Europe which exchanged coded internet messages. Twenty-eight other people had been arrested as part of operation "Magnesium" for various offences, of which 17 were convicted and imprisoned for between 6 months and 3½ years for fraud-related offences. Seven were detained for investigation by the Immigration Service", *Guardian*, 2nd April 2003.

[106] Lord Lloyd, *Inquiry into Legislation against Terrorism*, Chapter 7; Home Affairs Select Committee, Minutes of Evidence 11th March 2003, Lord Carlile of Berriew QC.

[107] House of Lords Debates: 19 June 2000, col. 111:
Lord Bach … Why not use the product of interception warrants evidentially? First, the current prohibition on the use of evidence has worked well since the Act came into force. The existing regime has stood the test of time and offers valuable protection to privacy, which an evidential regime would not.
Secondly—perhaps this is the main argument—in a fast-moving communications industry, it is vital that the existing capability is protected. Exposure of interception capabilities would or might educate criminals and terrorists who might then use greater counter-inception measures than they presently do. We believe that it is vital that the existing capability is protected and that the exposure of interception capabilities, which would result, as night follows day, from a repeal of the prohibition, would educate criminals and terrorists. They would certainly use greater counter-interception measures than they presently do and the value of interception as an investigative tool—it is a valuable investigative tool, particularly against the most serious criminals and terrorists—would be seriously damaged.

210. The Regulation of Investigatory Powers Act 2000 forbids the use of domestic intercepts in UK court proceedings. There is, however, no such bar on the use of foreign intercepts obtained in accordance with foreign laws. Nor is there a bar on the admission of bugged (as opposed to intercepted) communications or the products of surveillance or eavesdropping, even if they were not authorised and were an interference with privacy. There is no bar on foreign courts using British intercept evidence if the intelligence and security services are prepared to provide it.

211. Other than the Republic of Ireland we have not been able to identify any comparable country with such an extensive ban. In international operations (such as against al Qaeda) the USA has published details of its intercept capacity of landlines, mobile phones, satellite phones, diplomatic correspondence, and satellite intercept of foreign communications.

212. We understand the concerns of the intelligence and security services, which include not only the protection of sources and methods but also the need to ensure that interception for intelligence purposes is not impeded by the imposition of complex procedures to meet evidential requirements. We recognise that a balance has to be struck between the public interest in prosecuting particular cases and the public interest in maintaining the effectiveness of intelligence gathering techniques and capabilities. We consider, however, that the balance has not been struck in the right place if intercepted communications can never be used evidentially.

213. Relaxing the ban would not place an obligation on the prosecution to use intercepted evidence. We can also see the case for modifying the normal rules governing the disclosure of evidence so that, for example, the prosecution would not be obliged to disclose intercept evidence, or even its existence, unless they chose to rely on it. This would need to be done with care to minimise the risk of miscarriages of justice, but those risks should not be greater than under the present system where the prosecution is forbidden from disclosing intercepted communications, even if they are exculpatory.

214. Consideration could also be given to having different classes of warrants authorising the interception of communications, some allowing evidential use of the product and others not. This is the approach taken by some other countries (where interception by the police and investigating judges in particular can be used evidentially).

215. It is important that making intelligence available for prosecution does not compromise the collection and use of intercepted communications for intelligence purposes. We hope that the current review can devise a system which meets both needs.

For those reasons, we are not convinced that a change to an evidential regime would involve a rise in criminal convictions in any more than the short term. Criminals and terrorists would become "wise" to it.

[108] House of Commons Debates: 3rd March 2003, col. 588:
Mr. Blunkett: I see no reason at all why I should not tell the House that a consultation is currently taking place on whether there should be a change. There have been considerable differences of opinion among security, intelligence and law enforcement agencies in this country for many years as to whether that would be appropriate. Let me say this as carefully as I can. Anything that prevents the security services from being able to undertake the kind of work that leads them to pre-emptive action, and not just prosecution—or undermines that work—is deeply unfortunate. If people were to withdraw from their normal practice, or if they thought that by engaging in normal communications they would be subject to court action and therefore ceased—and that put us at greater risk—we would have gained nothing and lost much. We seek to achieve a balance.

Terrorism as an aggravating factor when sentencing

216. While there is general agreement that prosecution is preferable to the use of detention under Part 4, we have already noted[109] that the length of potential sentence could encourage the use of Part 4 instead.

217. Other countries have sought to address such difficulties by introducing counter-terrorism legislation that allows motivation to be taken into account in sentencing, to allow a longer sentence to be handed down when the objective of a crime is terrorism than when the objective of that same crime is, for example, self-enrichment.[110]

218. The most satisfactory way of dealing with suspected terrorists is to prosecute them. Where this is not possible, because of the absence of evidence which could be used in a conventional trial, the current approach is to prosecute for non-terrorist offences. We believe that it would be worth considering an extension to this approach which would in our view be preferable to Part 4. For example, **it might be feasible to:**

    a. **define a set of offences[111] which are characteristic of terrorism and for which it should be possible to prosecute without relying on sensitive material, but**

    b. **raise the potential penalty where it can be established that there are links with terrorism.**[112]

219. This type of approach has been used successfully in the USA's Racketeer Influenced and Corrupt Organization Act (RICO).[113] Similarly, France has sought to avoid the difficult problem of defining "terrorism" by focusing on a number of criminal activities listed in the Criminal Code (e.g., kidnapping, hijacking, extortion, certain IT offences, forming armed groups, possession of explosives, and money laundering) and supplementing them with an aggravating feature, namely posing a serious threat to public order by intimidation or terror, which leads to an increase in the available penalty.[114] There is a logic to this approach – namely that crimes committed by terrorists are not distinguishable from other crimes by their intrinsic nature but by their purpose.

220. This approach could be regarded as a structured extension of the judge's duty to consider past offences or aggravating factors when determining sentence. However, it would probably be preferable to send the case to a qualified group of specialist judges for sentencing in cases where an increase in sentence was sought on the grounds that the offence was linked to terrorism.

221. Options for establishing that an offence is associated with terrorism, which would not involve making sensitive information public, include:

    a. requiring only the production of objective information about involvement in terrorism (such as a previous conviction for a terrorist offence) without needing to establish any explicit link to the offence. This could be justified on the basis that the

---

[109] See paragraph 181.
[110] A Bill is currently before the Belgian Parliament which would take such an approach (*Projet de loi sur les infractions terroristes*). The Swedish Antiterrorism law no.146 2003 also sets a distinct sentencing tariff for "ordinary" offences when there is a terrorist link.
[111] Article 1 of the *European Council Framework Decision on combating terrorism* 2002/475/JHA of 13th June 2002 lists some offences of this type. See Annex E.5, at page 119.
[112] Article 4 of the *European Council Framework Decision on combating terrorism* provides for making custodial sentences for some of the offences described in the previous footnote heavier than those imposable under national law for such offences in the absence of the special terrorist intent. See Annex E.5: page 119.
[113] Title IX of the Crime Control Act of 1970 (18 U.S.C. §§ 1961-1968).
[114] See *Articles 421-1* to *421-5* of the *Code pénal.*

person convicted of the underlying crime would have known before committing it that there was a risk of a longer sentence than normal;

b. using a Special Immigration Appeals Commission-like procedure involving a security-cleared advocate to represent the accused's interests to establish the link;

c. requiring only a lower standard of proof (e.g., balance of probabilities) to establish that the offence was linked to terrorism.

222. There are possible objections to this approach (e.g., it seems odd to require lower standards of proof for a more serious offence, and evidence of past links with terrorism may not be a completely reliable indicator of current involvement). These would need to be addressed by proper safeguards. Nevertheless, although we would regard it as second best to conventional prosecution, we would have less difficulty with it than we have with Part 4, particularly if the add-on sentence for the association with terrorism was no greater than the sentence for the underlying offence.

223. There may be merit in providing for longer maximum sentences for ancillary offences, such as financial fraud, even in cases where prosecution for a terrorism offence is possible.

The merits of using an investigative approach in this specialised context

224. **Another approach to the problem of confronting the suspect with specific accusations and evidence, without damaging intelligence sources and techniques, would be to make a security-cleared judge responsible for assembling a fair, answerable case, based on a full range of both sensitive and non-sensitive material. This would then be tried in a conventional way by a different judge. In our view this approach could be well suited for use in this limited context.**

225. Variations on this approach are used in other countries. For example, in France the examining magistrate (*juge d'instruction)* hears witnesses and suspects, orders searches and authorises warrants. The magistrate's duty is to look for both incriminating and exculpating evidence.[115] Both the prosecution and the defence see the case file as the investigation proceeds and may request actions from the judge. If the *juge d'instruction* decides there is a valid case against a certain suspect, he puts the case to a court (presided over by a different judge). The case is then argued on the basis of evidence which the examining magistrate has assembled and which the parties have had the opportunity to contest. There are also hybrid systems. For example, in Scotland the procurator fiscal has an investigatory role as well as a prosecutorial one.

226. We do not envisage seeking to replicate another system in its entirety, but to use the underlying principles to devise a system that works in the context of the British legal system (just as the Special Immigration Appeals Commission was inspired by, and arguably improved on, a Canadian model).

227. This approach could mitigate two problems that arise in this context under the current system:

a. the risk that the process of prosecution will lead to the need to disclose sensitive material;

b. the risk that, under the complex rules on the admissibility of evidence, intelligence-based evidence may be excluded. (See footnote 84, page 50.)

[115] *Code de la procédure pénale*, art. L81.

Disclosure of material

228. It is an important principle under the British system of justice that all the available evidence must be produced in the presence of the accused at a public hearing with a view to adversarial argument. The defence normally has the right to see all potentially relevant material, even if the prosecution is not relying on it (because it may undermine the prosecution's case). The parties argue out the significance of the evidence in court, where the judge's role is effectively that of an umpire, and the jury decides whether the prosecution's case is made.

229. Making all potentially relevant material public might serve the interests of a fair adversarial trial, but it could undermine the public interest if it revealed intelligence sources or techniques and so impaired the ability to gather intelligence. Nevertheless, there is an obvious public interest in prosecuting terrorists. The challenge is to achieve this fairly without compromising intelligence.

230. The disclosure rules are complex, and there are exceptions. For example, the doctrine of public interest immunity (PII) enables the prosecution to withhold material where the trial judge is prepared to agree that the public interest in non-disclosure outweighs the defendant's interest in having full access to all the relevant material. In doing so, the judge is required to carry out a "balancing exercise", weighing the likely effects of disclosure against the need to ensure justice (which encompasses the potential relevance of the material to the defence). PII does not seem to be a complete answer in Part 4 cases because, by definition, sensitive information is so central to them. The judge would be obliged to apply the doctrine that the public interest in the fair administration of justice always outweighs that of preserving the secrecy of sensitive information where its non-disclosure may lead to an injustice[116] and in many cases the judge might order potentially exculpatory material to be disclosed.[117] The prosecution's only alternative to disclosure would then be to drop the charge.

231. An investigative approach would address the disclosure problem by putting a security-cleared judge in control of assembling a fair, answerable, case. Just as the procurator fiscal works closely with the police in seeking evidence, the security-cleared judge would need to work closely with the authorities to fill any gaps in the case. The Special Immigration Appeals Commission has commented on the way in which gaps in some of

[116] Archbold, *Criminal Pleading, Evidence and Practice* (e.g., 2001 edition paragraph 12-44e).

[117] House of Commons Debates: 12 December 2001, Column 921:
Simon Hughes: With regard to court procedures, first, does the Home Secretary accept that it is possible at any level for courts to sit in secret and that the Government can at any stage issue a public interest immunity certificate, which means that some evidence or information may not be revealed? …
Mr. Blunkett: Of course, the first part of the hon. Gentleman's question … involves the holding of proceedings in camera in a normal court and the evocation of public interest immunity to the point where not only the evidence that is presented would be protected, but those presenting it and those working on behalf of the security services. The security services made it absolutely clear to me—I do not think that I am breaching any confidence in saying this—that they would bring no cases forward if we used the normal court system and attempted to use public interest immunity.

the material before it could have been filled by further inquiry.[118] Putting an independent judge in charge of assembling the case could help address this point. It might also help to provide a systematic way of ensuring that exculpatory material was properly taken into account in the case.[119]

Admissibility of material

232. Information derived from intelligence may not be sufficiently robust to be admissible as evidence in adversarial court. A terrorist case may involve a myriad of small pieces of intelligence or assessments from which it may be difficult to draw inferences when they are considered individually, but which might be seen to form part of a consistent pattern of significance when looked at in the context of all the evidence.

233. This is a real issue: for example, hundreds of the US Government's exhibits against Enaam Arnaout[120] were thrown out by the court on the grounds that most were "hearsay" based upon unverified statements by co-conspirators. We face similar issues in the UK criminal justice system in the context of the general rule about the inadmissibility of "hearsay" statements.[121] The principle that the accused should be protected from information that cannot be properly assessed is a sound one under the adversarial procedure. The case for a blanket rule excluding hearsay from the proceedings is weaker under the investigative model because professional judges charged with protecting the suspect evaluate the information and give it the appropriate weight in the case, rather than being obliged to discard it completely.

234. The following table summarises the differences in the way that the adversarial and investigative approaches treat evidence to illustrate why the investigative approach may be better suited to cases involving sensitive information or information that may not be admissible as evidence under current rules:

[118] "52 … Sometimes the enquiries were not pursued for the simple reason that at the time of the investigation, there was no desire or need on the part of the services to do more than see whether a particular individual was of interest to them so that resources should be allocated to him; they were not as such collecting evidence and still less were they trying to prove a case or investigate a possible innocent explanation. It is not a question of them simply ignoring material which might assist the Appellants because their minds would not be deflected from the track upon which they were set. It is that by the nature of their habitual task, they deal with suspicion and risk rather than proof. So it does not always appear to them necessary to pursue lines which might confirm or eliminate alternative explanations. But it does mean that less weight can be attached than otherwise might have been the case to certain aspects which aroused their suspicions. There may be a gap, between a seemingly suspicious activity and it giving reasonable grounds for suspicion in this context, which cannot be filled by inference or assessment where it could readily have been filled by further investigation." Special Immigration Appeals Commission generic judgment SC/1,6,7,9,10/2002 (29th October 2003).

[119] See footnote 90 on page 52.

[120] *United States v. Enaam M. Arnaout*, sealed decision, 5th February 2003, Northern District, Illinois.

[121] We note that the Criminal Justice Act 2003 has recently extended the courts' discretion to admit hearsay evidence where it would not be contrary to the interests of justice for it to be used.

Table 2 The treatment of evidence under the adversarial and investigative judicial systems

	Adversarial	Investigative
Responsibility for conducting the investigation and assembling evidence	Prosecution and defence.	Investigating judge.
Disclosure of potential evidence	Very full disclosure of potential evidence presumed. Trial judge rules on disclosure of material for which public interest immunity is claimed.	Prosecution and defence presumed to have incentives not to disclose everything, so disclosure needs to be overseen by investigating judge.
Admissibility of evidence, to ensure that it is fair	Complex rules policed by trial judge.	Assessed by investigating judge.

235. **In our view, despite the obvious difficulties, it would be worth working up more detailed proposals for an investigative approach for the specialised purpose of handling terrorism cases, where conventional prosecution might risk disclosing sensitive sources, or the available intelligence might not be admissible as evidence.**

More structured disclosure rules

236. It is possible that, in some cases, the prosecution could be inhibited by the risk that it will be required to disclose sensitive information in the discovery process,[122] even if it is not relying on it, because it could help the defence.

237. The USA has a procedural statute called the Classified Information Procedures Act (CIPA). It does not change either the substantive rights of the defendant or the discovery obligations of the government. It is designed to balance the rights of a defendant with the interest of the state to know in advance the extent of the potential threat to its national security from pursuing a criminal prosecution. Each of CIPA's provisions is designed to prevent unnecessary or inadvertent disclosures of classified information and to ensure that the Government is in a position to assess the national security "cost" of proceeding with its case.

238. For example, to the extent that the court rules that certain classified material is discoverable, the prosecutor may seek the court's approval to use alternative measures such as deletion of sensitive information, substitution of summaries, closing the court, allowing witnesses to remain anonymous, requiring the defence to make its case known earlier in the process, and only allowing the defendant's security-cleared counsel to have access to the sensitive material.[123]

239. **Although the present public interest immunity rules in the UK already permit a certain amount of editing and summarisation there would, in our view, be merit in developing a more structured disclosure process that is better designed to allow the**

[122] Be subject to "graymail", in the legal vernacular.

[123] In April 2003 the Australian Attorney-General, Daryl Williams, asked the Australian Law Reform Commission to review measures to protect classified and security sensitive information used in the course of investigations and proceedings. The Review's background document contains a comprehensive account of the issues raised by the use of sensitive information in courts and tribunals of different types and in immigration hearings across a range of countries, including a discussion of CIPA. More information on the progress of the review can be found on http://www.alrc.gov.au.

reconciliation of the needs of national security with the rights of the accused to a fair trial.

Plea bargaining

240. At present it appears to be quite difficult for the police and security services to obtain information from a suspect, even in a case where the suspect might be willing to co-operate. The suspect's solicitor will usually advise the exercise of the right to silence, and there is no structured way in which to reach an accommodation which might crucially lead to the prevention or detection of more terrorism.

241. A plea bargain is an understanding between the prosecutor and the defendant (e.g., where the police agree to drop certain charges, or proceed on lesser ones in exchange for a guilty plea to other or lesser charges, or in return for information about the inner workings of a terrorist group such as membership, organisational structure, weaponry, and finances). This method has been used with some apparent success against terrorism elsewhere (e.g., the *penititi* in Italy and ETA in Spain and, more recently, extreme Islamist terrorists in the USA[124]). Laws permitting sentence reduction in return for co-operation exist in a number of countries.[125] Article 6 of the (Justice and Home Affairs) *Council Framework Decision of 13th June 2002 on combating terrorism*[126] provides for the reduction of penalties if the offender:

> *(a) renounces terrorist activity, and*
>
> *(b) provides the administrative or judicial authorities with information which they would not otherwise have been able to obtain, helping them to:*
>
> *(i) prevent or mitigate the effects of the offence;*
>
> *(ii) identify or bring to justice the other offenders;*
>
> *(iii) find evidence; or*
>
> *(iv) prevent further [terrorist] offences*

242. **Under current arrangements in England and Wales[127] the court is not party to plea bargains (although it is made aware of them and can volunteer disapproval) and any reduction in sentence in return for co-operation is at the discretion of the judge.**

243. **There may, however, be particular merit in terrorism cases in giving the suspect greater certainty of outcome in the event of co-operation by establishing a sentencing framework within which the accused may be sure of securing a reduced sentence in return for co-operation.** The merits of this approach were discussed by

---

[124] For example, the case of Iyman Faris, sentenced for 20 years in October 2003 for supporting al Qaeda and targeting the Brooklyn Bridge. http://news.findlaw.com/hdocs/docs/faris/usfaris603plea.pdf is the plea agreement.
The requirement to know the defence's case earlier in the process under the Classified Information Procedures Act can help facilitate plea bargaining.

[125] For instance, the Itialian "measures in favour of those who dissociate from terrorism" (*Misure a favore di chi si dissocia dal terrorismo*), law of 18th February 1987, no. 34; Article 579 of the Spanish Penal Code; Article 1 of the Turkish Remorse Law (Pismanlik Yasasi) no. 4450 of 26th August 1999 and Articles 61 and 62 of the Russian Criminal Code.

[126] See Annex E.5: page 119.

[127] For example, *R v Sinfield* 1981.

Lord Justice Auld in the wider legal context in his *Review of the Criminal Courts of England and Wales*.[128] Such a system would need to involve the supervision of the judge and to be implemented with a degree of sophistication: the discredited "supergrass" system in Northern Ireland in the early 1980s clearly illustrated the risks of injustice involved.

Surveillance

244. Surveillance is a vital component of an effective counter-terrorist policy. It is obviously important in detection and in the collection of evidence for successful prosecution.

245. It is also crucial in the prevention of terrorism (which is always preferable to prosecution after the event) because it can provide intelligence to enable terrorist activity to be disrupted, and gives leads to follow up in criminal investigations.

246. In particular, surveillance can help to spot indications of terrorists forming their organisations, recruiting, developing operational and logistical capabilities, and gathering information on potential targets. It can help to identify terrorists re-entering the country after training, uncover safe houses, identify arming and financing channels, and help to establish networks of informants.

247. The use of surveillance does, of course, have adverse human rights implications, as well as lacking the certainty of detention. Our view that more intense surveillance would, nevertheless, be preferable to Part 4 has been supported by evidence to the Committee.[129] The use of new technology may help to make surveillance more effective, although the use of more intrusive techniques requires adequate safeguards.

248. We have discussed this point with the appropriate authorities and are not convinced that enough use is made of the surveillance of suspected terrorists. As we have already noted, the Special Immigration Appeals Commission has pointed to the scope for further investigation.[130] We recognise that surveillance can be expensive. If the current degree of surveillance is unduly constrained by a lack of resources, we believe that the extra resources should be provided as a matter of urgency.

---

[128] See "Advance Indication of Sentence", pages 434ff, *Review of the Criminal Courts of England and Wales*, Lord Justice Auld, October 2001.

[129] John Wadham, Director of *Liberty*: "There are other ways perhaps of getting evidence against individuals, including, of course, surveillance, not just telephone tapping but all the other kinds of surveillance. The key issue for us is obviously to stop those people involved in terrorist activities. You require evidence and you require intelligence and I am not sure increasing those two key parts of what is required is going to be improved significantly by the Anti-terrorism, Crime and Security Act….
[T]he resources involved in [intensive surveillance] are considerable but that is better and would not require derogation from the Convention in the way that detention would. I do not know - because the Government has never said this - how much work the security services, the police and the Government have done in relation to alternatives to detention, listening devices, bugging, following people around, letting them know they are under surveillance or whatever. Those are more proportionate measures and would not require detention." Public hearing, 12th December, 2002, pages 8, 19.
Professor Conor Gearty: "…one is worried that in a way the anxieties of the security services would lead to a surveillance society…. But is not surveillance a new sort of word for good police work - intelligent penetration, which [Professor Wilkinson] was talking about earlier on, collection of forensic materials? It is not impossible to re-classify it and take away this ominous phrase "surveillance" and put in "good police work". Good police work is expensive as was established in Northern Ireland, catching people like Magee, the Brighton bomber, by completely conventional police methods. Forensics is painstaking and expensive and maybe this is something we cannot afford to run away from. " Public hearing, 12th December, 2002, pages 62-3.

[130] See footnote 118 on page 62.

249. As will be readily apparent from this Report, the need for additional resources is not a feature of our recommendations. We do, however, feel that **the Government should examine the scope for more intensive use of surveillance and we draw this view to the attention of the Intelligence and Security Committee, so that they can take account of it in their scrutiny of the intelligence and security agencies**. **We have in mind not simply the marking of particular individuals or groups, but also training, the use of technology and better liaison between different agencies at ports of entry.**

Other options

250. **It is possible that, even adopting some or all of the measures above, it may not be possible to prosecute in every case. The alternatives listed below would allow steps to be taken against both UK and foreign terrorist suspects which are less damaging to human rights than the current process (and so remove the need for derogation from the ECHR). These measures are less attractive than conventional prosecution and surveillance but in our view they are preferable to Part 4 as it stands.**

Restrictions on liberty

251. **The current Special Immigration Appeals Commission regime is used in cases which involve the detention of foreign nationals without charge. It would be less damaging to an individual's civil liberties to *impose restrictions* on**

a. **the suspect's freedom of movement (e.g., curfews, tagging, daily reporting to a police station);**

b. **the suspect's ability to use financial services, communicate or associate freely (e.g., requiring them to use only certain specified phones or bank or internet accounts, which might be monitored);**

subject to the proviso that if the terms of the order were broken, custodial detention would follow.[131] Such an approach is available in France[132] and in Sweden,[133] for example.

252. This would not necessarily be a suitable approach for every case (e.g., for those who were considered dangerous to the public), but it could be a more proportionate measure for some of those involved in supporting terrorists.

253. It would also make surveillance more effective where it was used.

Deportation

254. **In cases where deportation is considered the only possible approach — and we have considerable reservations about it as a way of dealing with suspected international**

[131] Arguably an unstructured version of this facility is already available under Part 4. The Special Immigration Appeals Commission has concluded (see, e.g., SC/3/2002 paragraph 9) that it would be possible for the Commission to grant bail if it was persuaded that certification was justified but to detain was disproportionate.

[132] See page 19 of *Rapport présenté par la France au Comité du contre-terrorisme en application du paragraphe 6 de la résolution 1373 du Conseil de Sécurité, en date du 28 septembre 2001* which refers to Articles 28 and 35bis of *Ordonnance n° 45-2658 du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France.*

[133] The Swedish and other examples are discussed in the Scottish Executive consultation document: *Tagging offenders; the role of electronic monitoring in the Scottish Criminal Justice System*, October 2000.

terrorists[134] **— we have seen no evidence that it would be illegal for the Government to detain the deportee while taking active steps in good faith to reach an understanding with the destination government to ensure that the deportee's human rights were not violated on his return. This is what some other countries seem to have been able to do, at least in some cases.**

255. Our view that the Government could take a more proactive approach in such deportation cases is reinforced by the observation that two of those certified under Part 4 as undeportable suspected international terrorists have been able to leave the country without apparently putting themselves at risk.[135]

256. We are aware that there has been at least one case[136] where the judges concluded that the assurances that the UK Government had obtained from the destination government did not, in the light of other evidence, provide a sufficient degree of reassurance about the safety of the deportee on his return. Such judgements do not, however, invalidate the principle of the approach.

257. **To supplement this approach, the Government could seek to establish framework agreements in advance with some of the main countries involved, to minimise the delay in dealing with individual cases. Even if deportation was rarely used in practice in terrorism cases, it might serve to act as a deterrent to international terrorists considering the use of the UK as a base for their activities.**

Other issues

Information

258. Representations have been made to us that it is difficult to obtain factual information about the use of counter-terrorism legislation. The media often give greater prominence to arrests than to subsequent releases without charge which can, over time, give a misleading impression of the impact of the legislation. We recommend that **the Government should publish up-to-date anonymised information on its terrorism website on:**

a. each Part 4 certification setting out its duration and current status, including the outcome of any appearance before the Special Immigration Appeals Commission including bail hearings or appeals (giving both the determination and a link to the full open reasons); and

b. the number of detentions that there have been under the Terrorism Acts and their outcomes (e.g., prosecution, certification under Part 4, release). Usage statistics for Part 4 are set out in paragraph 183ff. Table 3 gives recent figures for the Terrorism Act 2000.

---

[134] See paragraph 195.
[135] See footnote 98 on page 54.
[136] *Singh and Singh v Home Secretary* SC/4/99 SC/10/99, SIAC, 31 July 2000, where Mr Justice Potts concluded that "In future cases we would earnestly urge the [Home Secretary] to consider whether the type of material he relied upon in these appeals is sufficient to do justice to the case."

Table 3: Results of Terrorism Act 2000 investigations (1st November 2002-4th November 2003)[137]

Released without charge	126	45%
Sectioned under Mental Health Act	5	2%
Bailed to return	23	8%
Cautioned	4	1%
Detained by HM Immigration	32	11%
Terrorism Act 2000 charges	34	12%
Non-Terrorism Act 2000 charge(s)	35	12%
Terrorism Act 2000 charges and non-Terrorism Act 2000 charges	22	8%
Total	281	100%

Section 36: Destruction of Fingerprints

259. Section 36 is discussed on page 86, under Part 10 ("Police Powers").

[137] Source: Police. We understand that no detentions under Part 4 of the Anti-terrorism, Crime and Security Act 2001 arose from Terrorism Act 2000 arrests during the period.

D.5: Part 5 – Race and Religion

Background

260. The Anti-terrorism, Crime and Security Bill had included a new offence of incitement to religious hatred, which would have created an offence of inciting another person to commit a criminal offence on the basis of religious hatred, even if the other offence was not committed or even attempted.

261. The proposal had a mixed reception:

    a. Those opposing it felt that it might criminalise too wide a range of behaviour, including legitimate theological and artistic expression engaging with religious themes; that legislation in this field attempts to regulate behaviour touching on matters of personal faith or religious belief and consequently raises serious problems of principle, as well as practical problems of evidence; and that any such measure should be considered in a wider context, including such matters as the law of blasphemy and other religious offences;

    b. Those supporting the measure argued that current laws relating to racial hatred had the effect of protecting some religious groups but not others (including Muslims). They wanted to make it clear that all religious groups should be protected against the effects of religious hatred and discrimination.

262. It is clear that the proposed offence was intended to reassure the Muslim community that attacks against them following the events of Autumn 2001 were being taken seriously.[138]

Provisions

263. Given the specific difficulties raised by the proposed incitement offence, a compromise was reached. As a result, Part 5 is limited to extending the provisions dealing with racially aggravated offences in the Crime and Disorder Act 1998 (e.g., certain assaults and public order offences) to cover offences aggravated by religious hostility.

264. Under that Act, the listed offences are "aggravated" if there is evidence of hostility towards the victim by the perpetrator based on the victim's membership of a racial group. Where a court decides that there is evidence that they were motivated by religious hostility, sentences for these offences can, as a result, be increased.

Usage

265. The Part 5 provisions have had a modest effect, with 24 recorded convictions for religiously aggravated offences between December 2001 and October 2003. Most of these were of a public order character.

[138] House of Lords Debates: 27 November 2001, cols. 149-150: Lord Rooker "As to race and religion, the current international situation has been used to abuse people and we believe that it is right to extend the laws to protect our citizens from hatred based on religious belief. We have therefore brought forward four proposals…".

266. In the period 14 December 2001 to 17 October 2003, the CPS received 53 cases from the police. Of the 43 cases where an outcome had been reached:

    a. 24 resulted in a conviction for religiously aggravated crime;

    b. 3 resulted in conviction for the basic offence only;

    c. 16 resulted in an acquittal or were discontinued.

Our view

267. In our view, terrorism legislation agreed on an emergency timetable was not the appropriate context for measures that raised important and contentious matters of principle and expediency that merited careful deliberation. Even among Muslims otherwise supportive of measures against islamophobia the inclusion of the measure in emergency legislation addressing terrorism was considered inappropriate,[139] although it has also been said by some that repealing it in isolation would be undesirable.[140]

268. A Select Committee on Religious Offences in England and Wales was appointed to consider the subject of religious offences in general, on the basis of a recommendation by the Liaison Committee, following the introduction of Lord Avebury's Religious Offences Bill which had been presented to Parliament following debate on Part 5. The Select Committee has now had the chance to investigate the religious aggravation measure in the context of the wider issues raised by blasphemy and incitement to all forms of hatred.

269. The Select Committee reported in April 2003, having considered aggravation in this context. The report noted that the law of aggravation may have a deterrent effect, by denoting the particular unacceptability of islamophobia and religiously motivated violence of all kinds. It illustrated the difficulties raised by seeking to create offences based upon matters of personal faith and religious belief. For example, the Committee took the view that the existing aggravation offence raised serious difficulties for prosecutors.[141] The report illustrates the need for proper consideration of a measure which raises wider issues.

270. We are firmly of the view that violence based upon religious hatred is unacceptable. The need for new legislation in this sensitive area is, however, controversial for religious and political reasons. In these circumstances, and because any such measure has no place in terrorism and security legislation, we recommend that **the case for offences aggravated**

---

[139] Sadiq Khan, oral evidence to the Committee, 19th June 2003: "I think, it's not just cynics who would argue that the justification for the addition of these clauses was "a sop to the Muslim communities" but I think the Prime Minister and the Home Secretary, at the time, recognised that the increase in the number of Muslim victims of crime post 9/11 was startling. The Muslim News which is a monthly publication published some of the case studies of some of the people who had been assaulted post 9/11 which were horrific and in fact when Muslim leaders attended No 10 in October one of the things that the Home Secretary and the Prime Minister assured them was legislation to protect them. We were then shocked to see that legislation, as part of the emergency legislation to fight terrorism, because clearly that wasn't the place for it and you'll remember from the history that originally the subject of incitement to religious hatred was part of the Anti-terrorism, Crime and Security Bill and was consequently removed by the Home Secretary because of concerns about the problems of that being in this Bill/Act".

[140] "120. We would prefer to see these powers coming under a separate legislation which would deal comprehensively with incitement to religious hatred and crimes motivated by religious hatred. However, whilst there is a vacuum in existing legislation, we believe that Part 5, Section 39 should not be repealed as it is the only means of protection and legal recourse that Muslims have." *A submission from the Forum Against Islamophobia and Racism, May 2003.*

[141] Select Committee on Religious Offences in England and Wales Report, Vol.1, pages 35-6.

by religious hatred should be reconsidered in the context of broader mainstream legislation designed to protect the range of targets of hate crime.

D.6: Part 6 – Weapons of Mass Destruction

Purpose

271. The Biological Weapons Act 1974 and the Chemical Weapons Act 1996 implemented the provisions of the United Nations Biological Weapons Convention and the Chemical Weapons Convention,[142] both of which required amendments to the United Kingdom's domestic law. They established offences relating to the development and use of both categories of weapon. Part 6 brought uniformity to the criminal offences that had been created by those Acts and created similar offences relating to the development and use of nuclear weapons.

272. This restructuring of Weapons of Mass Destruction offences had first been proposed by the Government in a White Paper on Strategic Export Controls in 1998.[143]

Provisions

273. The Biological Weapons Act 1974 did not include an offence of transferring biological weapons agents outside the UK. Nor did it claim jurisdiction over actions by UK persons abroad. The Anti-terrorism, Crime and Security Act 2001 brought the biological weapons legislation into line with the provisions of the Chemical Weapons Act 1996 on both counts.

274. Previously, no specific offences relating to the making or use of nuclear weapons had existed, though such behaviour would have been criminal under other headings, notably the Explosive Substances Act 1883. Part 6 of the Anti-terrorism, Crime and Security Act created new specific offences of:

    a. knowingly causing a nuclear weapon explosion;

    b. developing, producing, or participating in the development of a nuclear weapon;

    c. possessing a nuclear weapon;

    d. participating in the transfer of a nuclear weapon;

    e. engaging in military preparations intending to use a nuclear weapon,

    in the United Kingdom or abroad (by a "UK person"), except where authorised by the Secretary of State or carried out in the course of armed conflict.[144]

[142] The Conventions came into force in 1975 and 1997 respectively.
[143] Cm 3989, July 1998, 3.1.
[144] No similar exemptions apply to Chemical and Biological weapons offences, reflecting the absolute prohibition agreed in the relevant UN Conventions.

Usage

275. There have been no prosecutions under this Part of the Act.

Our view

276. **No objections to this part of the Act have been brought to the Committee's attention. It seems to be an unexceptionable tidying-up of the legislation which in part fulfils our obligations under the UN Biological and Chemical Weapons Conventions.**

Application to foreign nationals

277. Questions have been raised about the definition of a "UK person" whom the Act would criminalise for undertaking the development, production, or use of chemical, biological and nuclear weapons abroad: debate in 2001 addressed whether it should be extended to include all persons domiciled in the United Kingdom, rather than just UK nationals.[145]

278. The Government chose in 2001 to limit the effect of the Act to full UK nationals, on the grounds that extraterritorial jurisdiction over foreign nationals can be problematic in circumstances where actions are criminal in the eyes of UK law even if they were carried out legally according to the law of the country in which they took place.

279. International terrorism is a special case however; this was recognised by the United Nations Convention for the Suppression of Terrorist Bombings (1997) which requires states parties to ensure that where bombing offenders cannot be extradited, they must be liable to domestic prosecution.[146] Accordingly, the Terrorism Act 2000 makes special separate provision for the prosecution of terrorists in the United Kingdom.[147] In effect, Weapons of Mass Destruction offences are liable to prosecution in the UK when carried out abroad by:

    a. "UK persons" (under the Anti-terrorism, Crime and Security Act 2001);

    b. persons in general, including foreign nationals, where the actions are carried out for the purposes of terrorism (as defined under the Terrorism Act 2000).

280. We are satisfied that the Acts taken together provide an appropriate framework for UK jurisdiction over Weapons of Mass Destruction offences.

[145] House of Commons Debates: 26th November 2001, cols. 718-9. The definition of "UK person" also includes a Scottish partnership or a body incorporated under UK law.
[146] A principle which is also set out in other UN conventions on terrorism, including the Convention for the Suppression of the Financing of Terrorism, 1999.
[147] Terrorism Act 2000 Section 62 extends jurisdiction in this way over offences under the Biological and Chemical Weapons Acts, and the Explosive Substances Act.

D.7: Part 7 – Security of Pathogens and Toxins

Purpose

281. Part 7 created a security regime for laboratories where pathogens and toxins are handled.

282. Previous legislation and regulation had only addressed the security of laboratories from a health and safety point of view. Laboratories were required to protect employees and the general public from the effects of accidents, but the legislation and regulations did not address the specific risk posed by the individual making a deliberate attempt to gain access to lethal substances with a view to inflicting harm.

Provisions

283. The Act requires laboratories to report all holdings of the materials listed in Schedule 5 (e.g., dengue fever virus, Ebola virus, and botulinum toxins) to the Home Secretary. It gives powers to the police to inspect premises holding such materials and to make security directions to their owners.

284. These directions can, if necessary, be enforced by the Secretary of State with reserve powers, including the enforced destruction of such materials if appropriate action is not taken.

285. The Home Secretary may also exclude any specified person from access to dangerous substances or the premises in which they are held. A Pathogens Access Appeals Commission is created for people aggrieved by such a decision.

286. The Home Secretary may add to the list of pathogens and toxins by statutory instrument under Section 75.

Usage

287. 310 premises notified the Home Secretary of holdings of Pathogen and Toxins under the requirement set out in Section 59 of the Act. Prior to the Act, the Health and Safety Executive were aware of only 50 such laboratories.[148] Police have embarked on inspecting and advising the large proportion of these laboratories holding the less dangerous, but still hazardous 'level 3' substances.[149]

288. 98 police counter-terrorist security advisers with appropriate training are now in place (as at 15th October) and have made initial assessments of 314 sites.

---

[148] Pathogens and Toxins Regulatory Impact Assessment, Home Office, 2001, see: www.homeoffice.gov.uk/docs/security_of_pathogens_and_toxins.pdf.

[149] The health and safety origins of the regulatory structure is clear from the definition of a "level 3" pathogen, which is classified as a biological agent that can cause severe human disease and may be a serious hazard to employees; which, furthermore, may spread to the community, but for which there is usually effective prophylaxis or treatment available. The group for instance includes anthrax and typhus.

289. No individual has had access to a laboratory suspended.

Our view

290. We are satisfied that the approach which the Act takes to regulation is a sensible one, where police can undertake the inspection of laboratories and consult directly with laboratory staff on security standards, avoiding the sort of bureaucracy that might be involved with a licensing regime, for instance.

291. This is however a technically difficult field and Parliament had only limited opportunity to scrutinise it under the Act's emergency timetable. Although the risk from insufficiently secure laboratories needed to be addressed, we believe that more time could have been given to preparation and consultation before legislation was presented and that this would have had no adverse impact on security; after 2 years, the regime for "level 3" laboratories is still not fully in place.

292. Since 2001, the police have had to develop a working basis for the inspection of laboratories in the absence of any preceding consultation, at the same time as developing their own expertise in a field for which they previously had no responsibility. Their work under difficult conditions has been commendable, and we welcome the fact that a dedicated corps of suitably trained police counter-terrorism advisers has now been established.[150]

293. The law is, however, only now beginning to have a real impact on some laboratories, including many of those handling "level 3" pathogens (see above); minimum security guidelines for those laboratories are to be published shortly.

294. **Some aspects of Part 7, which was subject to only very limited consultation, need to be urgently addressed.**

    a. **The list of relevant pathogens contained in schedule 5 (the so-called "Australia list") does not include all those materials which are of concern from a counter-terrorist point of view. The list in the Schedule should be amended to include all of these, as recommended by the House of Commons Select Committee on Science and Technology.**[151]

    b. **Evidence to the Committee has highlighted security concerns surrounding the holdings of some diagnostic laboratories. They should also be covered by the Act.**[152]

295. **Part 7 is only now beginning to have a direct effect: its further implementation should be subject to regular reporting to the Home Affairs Select Committee. We draw this matter to their attention.**

---

[150] Academic evidence to the House of Commons Select Committee on Science and Technology also noted the sensitivity with which the police had implemented the Act: Eighth Report, Session 2002-2003, November 2003, pages 59, 61.

[151] A more appropriate list, the "Salisbury list" has been in circulation for some time. "The confusion over the emergence of a second list of agents not covered under the Act is unfortunate… The Government seems to be under the impression that it can have one list of agents laid down in the Act, yet enforce another list which is beyond the scrutiny of Parliament. We recommend that the Government decide which organisms it wishes to control and amend the Act accordingly," Eighth Report, *The Scientific Response to Terrorism*, November 2003, 61.

[152] They are all exempted by the Security of Pathogens and Toxins (Exceptions to Dangerous Substances) Regulations 2002.

296. **The security of pathogens and toxins in the post and in transit is being addressed as part of the present inspection and consultation process by counter-terrorist security advisers; where possible, it is desirable that security should be built on the foundation of close consultation and co-operation between inspectors and laboratories. However, evidence to the Committee indicated that there are no relevant security (as opposed to health and safety) regulations for postage and transport; we believe it would be consistent with the rationale for Part 7 of this Act if police counter-terrorist security advisers were given statutory powers to enforce security provisions for the carriage of Schedule 5 pathogens and toxins where necessary.**

D.8: Part 8 – Security of Nuclear Industry

Provisions

297. Part 8 of the Act creates a new regulatory regime for the nuclear industry, strengthens provisions against the disclosure of sensitive information relating to nuclear sites, and extends the jurisdiction of the United Kingdom Atomic Energy Constabulary (UKAEC).

Usage

298. The Act has been applied in the following ways:

    a. after a period of consultation, the *Nuclear Industry Security Regulations* statutory instrument,[153]designed to update and consolidate security regulation in the UK civil nuclear industry, came into force on 22nd March 2003;

    b. there have been no prosecutions for disclosure of sensitive security information;

    c. the UKAEC have used their new powers to act as constables within 5km of nuclear sites on a daily basis.

Our view

299. We are satisfied that the measures contained in this Part are useful additions to the previous security arrangements for the nuclear industry.

Regulatory regime

300. The previous regime was, in the words of the DTI, "unsatisfactory, outmoded, lacking in transparency, contained a number of gaps and anomalies and saw security in different parts of the civil nuclear industry regulated on the basis of different, sometimes inconsistent statutes."

301. We have no difficulty with the thrust of these provisions, which seem to us to represent an unexceptionable and overdue modernisation of the regulatory regime governing the civil nuclear industry.

Disclosure of information

302. Sections 79 and 80 strengthen sanctions against the unauthorised disclosure of sensitive information on the security of nuclear sites, nuclear material and uranium enrichment nuclear technology.

303. At the time of the passage of the Bill, disquiet was expressed about the character of these offences, and the absence of an explicit exception or defence for disclosures made in the

[153] SI 2003/403.

public interest, for example to alert people to the existence of a danger to public health from the escape or negligent handling of nuclear material.

304. The Government argued that the offences are focused on the specific mischief that they address, and that they could think of no circumstances in which it would be in the public interest to disclose information that might prejudice the security of a nuclear site or of nuclear material.

305. More specifically:

    a. Section 79 does not prevent disclosures of information unrelated to security (e.g., safety or health or inefficient working practices);

    b. The introduction of a public interest defence would have been inconsistent with the objectives of the provision. To ensure their security, it is essential to protect detailed information on the routes of nuclear transports, time schedules, and the nature of the material being transported;

    c. The restrictions on the freedom of expression are proportionate and the minimum necessary to protect information about the security of nuclear sites and material, which is vital in the interests of national security;

    d. A great deal of available information relating to nuclear transport has no security implications (e.g., because it relates to past events).

    e. Two safeguards act as a check on inappropriate prosecutions:

        i. The consent of the Attorney General[154] is needed before any prosecutions can be brought under Sections 79 and 80;

        ii. For an offence to be committed under Section 79 there has to be an intention to prejudice the security of a nuclear site or of nuclear material or recklessness as to whether that security might be prejudiced.

306. With these assurances, we see no reason to object to these provisions.

Jurisdiction of United Kingdom Atomic Energy Authority Constabulary

307. Part 8 extends the jurisdiction of the United Kingdom Atomic Energy Authority Constabulary (UKAEAC). They can be deployed in all civil licensed nuclear sites and within 5km of such sites. They also have powers to escort nuclear material, and to prevent its theft.

308. These powers seem sensible modernisations. We welcome the fact that legislation has now been proposed reconstituting the Constabulary as a stand-alone force with a statutory Police Authority.[155]

Other radioactive sources

309. The provisions of Part 8 address those parts of the nuclear industry which are subject to regulation by the Office of Civil Nuclear Security. We note that other "non-nuclear" sources, i.e., radioactive sources which are held in areas not designated as "nuclear sites"

[154] Or that of his equivalents elsewhere in the UK.

[155] Managing the Nuclear Legacy: a Strategy for Action, Department of Trade and Industry, Cm 5552, 4th July 2002: www.dti.gov.uk/nid/nuclearlegacy/whitepaper.htm.

are not subject to specific counter-terrorist regulations, despite the risk of their use in a "dirty bomb". They include radiation sources in hospitals, others in university and research establishments, and those used to test the integrity of equipment in industry.

310. We understand that inspections assessing particular terrorist vulnerabilities at such non-nuclear sites have been taken forward since 2001 on a non-statutory basis, but it is not clear why the police should not be given the enforcement powers that they have elsewhere. **Existing regulations for non-nuclear radioactive sources only allow for the enforcement of health and safety regulations[156] (as with the provision for the handling of pathogens and toxins in laboratories before this Act[157]) and are not designed to prevent intrusion by an individual seeking to use radioactive material with a view to causing deliberate harm. We believe that this gap should be filled.**

311. **We believe that the security of radioactive sources should also be the subject of an annual report to Parliament, including information on any losses, and subject to further scrutiny by a Select Committee. Responsibility for this area is shared between a number of Departments, and we believe that the House of Commons Science and Technology Committee would probably be the most appropriate.**

[156] Most importantly the Radioactive Substances Act 1993, and the Ionising Radiations Regulations 1999.
[157] See Part 7 above.

D.9: Part 9 – Aviation Security

Provisions

312. Part 9 of the Anti-terrorism, Crime and Security Act 2001 amended the existing aviation security and related police legislation in four ways:

    a. it increased the powers of the police to arrest and remove intruders from the "restricted zone" of airports;

    b. it enabled the Government to make arrangements for maintaining a list of providers of security services to civil aviation that are approved to offer secure services (e.g., companies contracted by airports to provide passenger and baggage screening services and companies providing aviation security services);

    c. it introduced a power for Department of Transport Inspectors to detain aircraft where they have serious security concerns;

    d. it created an offence of falsely claiming to have been approved by the Secretary of State as a secure cargo agent.

313. The provisions form part of a wider range of initiatives that have been introduced to tighten airline security since 2001, including:

    a. regulations which were introduced separately in response to the 11th September attacks requiring for instance that cockpit doors be locked during flights, and prohibiting the use of metal cutlery on flights;

    b. Sir John Wheeler's review of provisions for the policing of airports and the security surrounding access, and persons with regular access, to the 'restricted zone' at airports.[158]

Our view

314. **Part 9 provides useful powers for tightening security at airports. They address certain threats to aviation from organised and other crime, including terrorism. They should, therefore, be revisited in the context of wider mainstream transport security legislation when a suitable legislative opportunity arises.**

Trespass and powers of arrest

315. Sections 82, 83 and 84 created powers for the police to arrest and remove suspects in cases of unauthorised presence in the restricted zones of airports, and increased the penalties for such intrusions.

[158] Sir John Wheeler, *Review of Airport* Security, September 2002. Evidence to the Committee has confirmed that his Review has resulted in a significant positive change in the way in which security and law enforcement authorities at airports co-ordinate their efforts.

Usage

316. The use of the new police powers is not subject to mandatory reporting, but 13 uses of the power of arrest were reported to us by police at Heathrow. There has been one successful prosecution for trespass.

Our view

317. The powers have been used, and evidence to the Review has confirmed that the police would otherwise have no statutory power to remove suspects in cases of unauthorised intrusion (the majority of which have no connection to terrorism).

Powers to detain aircraft

318. Section 86 enables Department for Transport inspectors to detain an aircraft where there are concerns about the standards of security applied, or prevent it from flying where there is good reason to believe it might be the target of an attack.

Usage

319. No aircraft have been detained or prevented from flying under these powers.

Our view

320. On those occasions where flights have had to be suspended following terrorist alerts since 2001, no such intervention has been necessary as operators generally have been responsive to such security concerns. Circumstances where an operator has proceeded with a flight against an inspector's advice have arisen in the past, however, and we are satisfied therefore that inspectors should have this enhanced power for such a contingency. Debate in 2001 raised concerns about the absence of mechanisms for appeal for operators whose aircraft had been detained: the Government argued that this would be unnecessary for a power intended only for serious emergencies. In the light of practice since 2001, we are inclined to accept this view.

Secure air services

321. Before Part 9, the Government could maintain a list of cargo agents who were accredited to provide secure air cargo services.

322. Section 85 enables the Government to maintain a similar list of companies providing security services to civil aviation (for instance, baggage screeners).

323. Section 87 enables the Government to prosecute in cases where air cargo agents falsely claim to have been accredited as secure by the Secretary of State.

Usage

324. Consultation on the regime for listing security companies was completed in 2002. Listing is now being carried out on a voluntary basis while a statutory instrument is developed in parallel.

325. There have been 3 cases of false claims to be security approved cargo agents. One resulted in a police caution and two in formal warnings by Department for Transport aviation security inspectors.

Our view

326. We have no difficulty with these measures.

Other comments

Part 13: Advance Passenger Information

327. Part 13 of the Act also provides for transport security. The Terrorism Act 2000 enabled police to request information from the owners of a ship or aircraft about passengers, crew or vehicles in the Common Travel Area (i.e., in relation to journeys within the British Isles). Section 119 extended this power to cover any passenger ship or aircraft arriving in, or leaving from, any place in the United Kingdom. A statutory instrument was passed in 2002[159] setting out the information that should be provided by operators on request.

328. The police report continued problems in getting access to such information in many cases.[160] Airlines and ferry operators have on occasion cited practical, data protection and financial barriers to providing the information, but it would appear that these objections have not prevented the provision of similar information to U.S. authorities. Good manifest information can be of crucial benefit in counter-terrorist operations, as Lord Carlile has also commented in relation to the Terrorism Act.[161]

329. **In our view, urgent consultation with air and ferry operators is required regarding the provision of advance passenger information under Section 119 of the Act.** We have been told that further non-statutory guidelines are forthcoming; **the Government should report during debates on this Committee's report on the steps that it has taken to increase compliance with the legislation.**

Other matters

330. **No fundamental concerns with the present primary legislation for aviation security generally were brought to our attention, but we should note some specific security issues which were raised with us.**

a. **In the light of the attacks of 11th September 2001, extensive attention has been given to controlling the entry of individuals and their hand luggage at points of access to the restricted zone of airports. Less attention has been given to access by cargo and other goods at other points of entry to the zone: for instance, to the checking of security seals placed on vehicles off-site. It is important that the extensive efforts that have been made to enforce security at points of access within the main airport buildings should not be undermined in this way.**[162]

b. **Lord Carlile commented in his report on the Terrorism Act 2000 on the inadequacies of Special Branch accommodation at some air and ferry ports, resulting in practical difficulties for the interrogation of suspects. We were told that steps were in hand to remedy the space restrictions, but the Committee's visit to Heathrow confirmed that better facilities are still required. This is a matter for the Home Office and airport operators.**

---

[159] The Terrorism Act (Information) Order 2002.

[160] The proposals presented in the Queen's Speech which would criminalise the destruction of travel documents and require airlines to copy them are relevant here.

[161] *Report on the Operation in 2001 of the Terrorism Act 2000*, pages 35-36.

[162] Recent reports suggest that the Al Qaeda network might be planning to use cargo planes in the manner of the 11th September attacks: press reports, 8th November 2003.

c. **Police specialising in terrorist and national security operations have experienced difficulties with the new personal search regime which applies to all people with access to the restricted zone, including airline and control staff. It has endangered a number of sensitive operations being conducted by Special Branch officers. It is desirable that all staff should be subject to the regime, but some means of relaxing controls in this very specific category of operations should be devised**.

331. We draw these matters to the attention of the Transport Select Committee.

D.10: Part 10 – Police Powers

Background

332. Part 10 amends several areas of police law affecting the rights of those in custody, the rights of the citizen generally, and the jurisdiction of two specialised police forces. The Government argued in 2001 that all these measures were justified on the grounds that they would be of direct benefit to the police in countering terrorism.

333. Some of these provisions appear to have been included in counter-terrorist legislation in order to take advantage of its accelerated passage and limited scrutiny, in order to avoid the difficulties which had previously been experienced in securing Parliamentary approval.[163] This inappropriate "fast-tracking" undermines the consensus which is desirable to allow legislation to be enacted rapidly in emergencies.

334. **Most of the reported uses of the Part 10 powers have not been related to counter-terrorism. While some of the measures have intrinsic merit,[164] they should be submitted again when the underlying legislation is next revised. Other provisions present an intrusion into individual rights which are not justified by any counter-terrorist benefits and should either be repealed or significantly amended.**

Identity theft

335. Sections 89 to 93 relate to the identification of people in custody.

336. The role of identity fraud in facilitating and financing contemporary terrorism was raised repeatedly in evidence to the Committee. **We were struck by the extent to which terrorists use crimes of "identity theft", involving the use of false personal documentation, as a basis for their operations. The falsification of identity documents enables them to evade detection,[165] circumvent immigration controls, and raise funds illegally.[166] This is a serious issue; however we are not convinced that all the relevant measures in Part 10 address it effectively.**

---

[163] In particular, comparable provisions relating to the jurisdiction of the Ministry of Defence Police were included in the Armed Forces Bill in 2002, but ran into opposition and were dropped in order to secure passage of the rest of the Bill in the time permitted. It is to be welcomed that the Defence Select Committee was able to bring special scrutiny to bear on these measures during debates on the Anti-terrorism, Crime and Security Bill.

[164] Notably, the provisions regarding the jurisdiction of the Ministry of Defence and British Transport police forces.

[165] For instance, a training manual found by the Manchester police during the search of an al Qaeda member's home, devotes two pages to the handling of falsified passports and identity cards. See www.usdoj.gov/ag/trainingmanual.htm.

[166] Jean-Louis Bruguière (*Premier Vice-Président chargé de l'instruction*, Tribunal du Grand Instance, Paris) noted the importance of credit card fraud as a basis for "micro-finance" in contemporary terrorism: "The numerous investigations carried out in France on [current terrorist] networks over a number of years have adduced the fundamental role played by [petty] crime in their funding. These activities range from the trafficking of forged documents or stolen cars to burglary and the swindling of state institutions... But probably the fraudulent use of credit cards with the so-called "cloning" method is the most lucrative one – it has been estimated that such an activity could provide over 200,000 francs a week to its perpetrator," speech: *The Financing of Terrorism*, Munich 2001.

337. Evidence from the police highlighted the practical difficulties that they face in investigating cases where there is a suspicion that an individual is engaged in these activities; we were told that powers of search and detention in these cases were inadequate. We welcome the fact that the Criminal Justice Act has put the offence of fraudulently obtaining a driving licence on the same basis as fraudulently obtaining a passport. The Criminal Justice Act also makes both offences arrestable, which is an important basis for further investigation.

Measures to identify persons in custody

338. Part 10 enhances the powers of the police to take measures purely to help establish the identity of a person in custody— powers which previously were limited. The relevant sections[167] (which are complex) amend:

    a. the Police and Criminal Evidence Act 1984 (PACE) and corresponding Northern Ireland legislation, allowing police:

        i. to search and examine a person under detention to:

            (1) ascertain whether he has any identifying mark on him which might identify him as an individual involved in the commission of an offence; or

            (2) facilitate the ascertainment of his identity;

        ii. to take fingerprints using reasonable force where they will facilitate the identification of the person;

        iii. to take photographs, and to remove face coverings (including face paint) in order to be able to take useful photographs;

    b. the Terrorism Act 2000, allowing the police to take fingerprints from those detained under the Act in order to ascertain their identity.

339. The Act also enables the police to retain all photographs and fingerprints taken under these powers for the purposes of the prevention and detection of crime.

Usage

340. Use of the powers has not been systematically recorded. The details of a small number of specific cases have been reported to us; for instance, one incident involved the use of the search and examination powers on a Terrorism Act 2000 detainee.

Our view

Amendments to the Police and Criminal Evidence Act 1984 (PACE)

341. The measures significantly extend the circumstances in which fingerprints can be taken by force, for instance, which was previously only permitted:

    a. when persons were convicted or charged or cautioned for a recordable offence; or,

    b. where there were reasonable grounds to suspect their involvement in a criminal offence and fingerprints would tend to confirm or disprove it.

[167] Anti-terrorism, Crime and Security Act, Sections 89 to 93.

342. Police now have substantial powers of arrest under the Terrorism Act 2000, and for the fingerprinting of terrorism suspects following the Part 10 amendment to it. Together, these powers provide an acceptable basis for dealing with the specific problem of identifying people who are suspected of terrorism.

343. Their usefulness in relation to other crimes is more difficult to assess. In 2001, the Government resisted limiting the use of these powers to terrorist cases on the grounds that even where there are initially no grounds to suspect involvement in terrorism, such an identity check might establish that one exists. However, amongst the cases that were reported to us, none of the uses resulted in the identification of terrorists who had been in custody for other reasons; the majority involved individuals who had been detained under the Terrorism Act in any case.

344. The precedent that fingerprints might be retained in cases where the persons concerned have not been found guilty of an offence was established in the Criminal Justice and Police Act 2001 (and has since been extended in the Criminal Justice Act 2003).[168] It was controversial, and ought not to have been extended in emergency legislation.

345. **In our view, the privacy of innocent citizens who are subject to the Part 10 procedures should be protected. Those subsections enabling the police to retain fingerprints and photographs should be amended, permitting retention only in those circumstances where the subject is charged with an offence,[169] or where appropriate authorisation is given that they are of ongoing importance in a terrorist investigation.**

Amendments to the Terrorism Act

346. **The Terrorism Act 2000 provided no powers to fingerprint in circumstances where there was a reasonable suspicion of involvement in terrorism, but not of involvement in a specific offence. Section 89 fills that gap. This is an important amendment in view of the role of identity theft in terrorism. The power should however be subject to the same retention safeguards as the parallel powers contained in the Police and Criminal Evidence Act 1984.**

Other fingerprinting provisions: Part 4

347. The Act included another fingerprinting provision under Part 4, Section 36. The Explanatory Notes describes it as follows:

> *Section 141 of the Immigration and Asylum Act 1999 allows fingerprints to be taken in certain circumstances relating to immigration and asylum. Section 143 requires the fingerprints to be destroyed in a certain time. Section 36 removes this requirement, both for fingerprints taken in future and ones already held. Such fingerprints will now be retained for 10 years.*

348. The effect of Section 36 is to remove the previous requirement that the immigration authorities should destroy fingerprints once they had met their purpose: for instance, once the individual concerned had been given indefinite leave to remain, or their identity

[168] The Criminal Justice Act 2003 enables police to use force in fingerprinting and getting DNA samples from **all** those who have been *arrested* on suspicion of having committed (as opposed to having been charged with) a recordable offence. These could then be retained in all circumstances for the prevention and prosecution of crime.

[169] This would restore the circumstances in which they can be retained to those agreed by Parliament in the Criminal Justice and Police Act 2001.

as a UK or Commonwealth citizen with a right of abode had been established. As a result, all fingerprints taken for immigration purposes can be retained for ten years, purely on the grounds that they might be useful to a criminal investigation at a later stage. We note that this would even apply to UK citizens where the fingerprints had been taken to confirm their identity.

349. In 2001, the Joint Committee on Human Rights commented:

> *we are not persuaded that it is proportionate to treat all immigrants' fingerprints as being on a par with the fingerprints of those detained by the police. It seems to us to risk stigmatizing immigrants who have no criminal connections. The provision has no clear connection with terrorism or security. We recommend that the provisions should be reconsidered, and draw them to the attention of each House.*[170]

350. **The Section 36 provision that fingerprints taken under immigration powers can be retained for 10 years under all circumstances also gives rise to privacy concerns, and its justification on counter-terrorist grounds is not clear. We believe that the previous position on retention of fingerprints should be restored, except where appropriate authorisation is given that the fingerprints are of significance in an ongoing terrorist investigation.**

Power to remove disguises

351. Part 10 also extended the power of the police to remove and confiscate disguises (under Sections 94 and 95). These are separate powers, applying to the public more generally during public order incidents, rather than to those in custody. The Act amended the Criminal Justice and Public Order Act 1994, relaxing controls on the circumstances in which the powers could be used in two ways:

a. the officer who has the power to authorise such action by constables is of a lower rank than previously;

b. the circumstances in which the powers might be activated were broadened, from those where incidents involving "serious violence" are likely to occur to those where "offences" in general are likely to occur.

Usage

352. Use of these powers has not been reported systematically: two incidents have been brought to our attention, however, where they were directed at hunt saboteurs. Suspicions that the powers were designed to target Muslims wearing hijab would appear to have proved unfounded but, to date, so has the Government's argument in 2001 that the powers would prove useful against masked terrorists exploiting demonstrations as a cover for their own operations.[171]

---

[170] Second Report, 2001-2 Session, page xv.

[171] House of Commons Debates: 27th November 2002, col. 760: Beverley Hughes "…the police believe that the tactic of wearing face coverings has become increasingly widespread during all kinds of events that could lead to public disorder. The circumstances in which the police believe that they may be able to predict serious violence are also much wider than that. Furthermore, the circumstances in which people use the tactic of wearing face coverings to hide their identity and want to use the camouflage that a big public event might give them as a vehicle for terrorist activities are much wider than was hitherto thought to be the case."

Our view

353. These amendments considerably enlarged the range of circumstances where the power to remove disguises might be used. We see no justification for the double extension of the power discussed above (see paragraph 351), and we are concerned about the absence of safeguards against abuse.

354. **We believe that the previous limits on the general circumstances where the police are entitled to demand the removal of disguises should be restored. We are however satisfied that a more strictly defined power should be retained for those cases where a senior police officer believes that this measure is necessary in response to a specific terrorist threat.**

British Transport and Ministry of Defence Police: extended jurisdiction

Provisions

355. Finally, Part 10 extends the scope for action by the British Transport and Ministry of Defence Police (BTP and MDP) in emergencies and on request outside their pre-existing jurisdictions.

356. It gives officers of the British Transport Police and the Ministry of Defence Police the usual powers of a police constable to act in emergencies where an officer from the local force cannot be contacted in time, and where ad hoc assistance is requested from them by local police forces.

357. This broadened the statutory basis on which the two forces might deal with the wider public outside their core jurisdictions on the railways and defence estate.

358. Part 10 also enables the Ministry of Defence Police to provide pre-arranged mutual aid support to other forces on request, under the command of the requesting Chief Constable.[172]

Usage

359. Our work has been made easier by detailed reporting from both forces on the use of the powers. By 31st August 2003, the British Transport Police report 2,512 cases where arrests or other interventions had been made outside their previous jurisdiction. The Ministry of Defence Police report 3,918 uses of the powers by the same date.

Our view

360. The measures gave rise to fears that the forces (particularly the Ministry of Defence Police) might develop a permanent role in routine police work beyond the ad hoc circumstances defined by the Act, and that this extended role with the public would not be governed by some of the existing checks that apply to the other conventional police forces, including provision for public oversight, independent inspection and independent complaints-handling.[173]

[172] Unlike operations under the other Part 10 powers, where MDP officers remain under the command of their own Chief Constable.
[173] See paragraph 365ff below.

361. Both Forces have taken the limits on their new powers seriously. The great majority of the uses have arisen in routine policing contexts and have been of clear benefit to the public. The ability to respond to requests from local forces has proved beneficial: for instance, the British Transport Police have been able to provide public order support to local forces policing football-related disorder from their strategically important base on the railways. Furthermore, members of the public frequently look to uniformed officers of both Forces to perform the normal duties of policemen in circumstances which were not provided for outside their previous jurisdictions. Before 2001, they had no statutory basis for taking any such action,[174] even in emergency cases where officers from the local constabulary could not be notified in time. Using the powers which apply when local forces cannot be notified, the Ministry of Defence and British Transport Police have been able to deal with a wide range of routine incidents encountered in the course of their duties when police from the local constabulary were not at hand.

362. **In our view, it is desirable in the limited circumstances set out in Sections 98 to 101 that constables of the British Transport and Ministry of Defence Police should be able to act with all the authority of "Home Department" constables. We support the extension of the jurisdiction of both forces, but believe that it should be revisited when the underlying legislation is next revised.**

363. The Defence Select Committee registered its concern in 2002 that the Ministry of Defence Police might be developed as an armed counter-terrorist national reserve under the Section 99 provisions for mutual aid.[175] The Government has since said that there is no intention to develop the force in this way, and we have received further assurances from the Government and the Ministry of Defence Police to this effect.

364. **Given the special character of the Ministry of Defence Police, however, it is important that the details of any mutual aid operations should be recorded and reported to Parliament. We welcome the Chief Constable's undertaking to provide an annual operational report in addition to the report and accounts required of him as Chief Executive of the Agency. The report should include detailed information regarding operations undertaken under Section 99.**

Accountability and other safeguards

Complaints and Inspection

365. In 2001, the Government undertook to enhance the public oversight of both forces as a safeguard against misuse of their new extended powers for work with the public.[176]

366. The Police Reform Act 2002 has introduced some significant improvements to the public scrutiny of both forces:

    a. complaints can now be handled by the Police Complaints Authority; and,

    b. provisions for independent inspection by Her Majesty's Inspectorate of Constabulary are now the same as those for other police forces.

[174] But frequently felt obliged to do so using the ordinary powers of the citizen, leaving officers open to civil suits.
[175] Defence Select Committee, Sixth Report, 2002.
[176] House of Commons Debates: 26 November 2001, col. 799, Lewis Moonie.

Public accountability

367. The institutional arrangements for public accountability are not straightforward for either force, since neither serves an obvious constituency in the way of the local ("Home Department") police forces, where public accountability is assured through the inclusion of local government representatives on Police Authorities. Both forces owe their primary duty to the bodies that they serve, and that fund them, namely the railway industry and the Ministry of Defence.

368. The creation of a British Transport Police Authority by the Railways and Transport Safety Act 2003 has put the force's accountability on a surer foundation. The balance of representation on its predecessor, the British Transport Police Committee, was tilted towards the interests of the rail industry, with 5 representatives of the industry and 4 lay people. It is welcome that the proportion of external voices on the Authority will be increased.[177]

369. We recognise the strong counter-terrorist record of the British Transport Police. The railways have historically been a primary target of terrorist action, and the force reacts routinely to bomb threats in a measured way, causing minimum disruption on the basis of an informed risk assessment.[178] Their role is integral to any strategic approach to the terrorist threat in the centre of our major cities.

370. We are satisfied that the Government's commitment to put accountability for the British Transport Police on a surer footing has been fulfilled.

371. It is appropriate that arrangements for accountability for the Ministry of Defence Police – whose responsibilities relate primarily to policing the defence estate – should reflect its primary duty to the Ministry of Defence. Accountability is managed by the Ministry of Defence Police Committee, reporting to the Secretary of State for Defence, and ultimately to Parliament.

372. Within these constraints, however, independence from the Executive needs to be maximised. The structure and working methods of the Ministry of Defence Police Committee have been revised since 2001, including the appointment of a new independent member. It has made some progress from being a purely administrative body to one capable of independent oversight.

373. **We recommend that future appointments of independent members to the MoD Police Committee (including the representatives of the appropriate trade unions and forces' family associations) should be subject to the Code of Practice of the Commissioner for Public Appointments, including public advertisements of the vacancies. We also take the view that, in the interests of independence, the Chairman of the Committee should be drawn from outside the armed services and the Ministry of Defence, and the appointment should be subject to the same procedure.**

[177] The Authority is due to start work on 1 July 2004, with the following membership: 4 industry representatives, 4 passenger representatives, 1 Strategic Rail Authority nominee, 1 representative of the rail unions and 3 regional representatives.

[178] Over the last decade, the British Transport Police dealt with 7000 bomb threats; only 1% of these resulted in station evacuation. Of this 1%, one half resulted either in an explosion or in the discovery of an explosive device.

D.11: Part 11 – Retention of Communications Data

Background

Communications data

374. In this context communications data is data relating to telephone, internet and postal communications (e.g., phone numbers, location data, call durations, e-mail addresses, websites visited, and subscriber information). It does not include the substance of the communication.[179] Such data allows investigators to identify suspects, examine their contacts, establish relationships between conspirators and place them in a specific location at a certain time. It is therefore clearly potentially useful for the prevention and detection of terrorism (among other crimes).

Retention of communications data

375. EU and UK legislation flowing from Article 8 of the ECHR (the right to privacy)[180] requires that communications data is retained only for certain specific business purposes (the management of billing or traffic, customer enquiries, the prevention or detection of fraud, and marketing). Otherwise it must be erased or anonymised, subject to a range of permissive public interest exemptions (e.g., where retention is necessary for national security purposes or for the prevention or detection of crime).

376. Retention requirements vary internationally. For example, the USA, which hosts some of our larger internet service providers, has no comparable destruction or retention requirements. The European Commission has reported:[181]

> *… Traffic data may be processed only for the purpose of billing and interconnection payments, up to the end of the period during which the bill may be lawfully challenged or payment may be pursued. …*
>
> *It is clear that the periods during which operators need to store traffic data for billing purposes vary considerably between Member States, since the period during which a bill can be lawfully challenged is usually based on civil law, which itself varies significantly; it ranges from three months (Finland) to six years (United Kingdom). This may create obstacles for the functioning of the internal market.*

[179] Accessing the substance of communications is referred to as "interception" and not relevant to Part 11.
[180] The retention of communications data is subject to Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications which interprets the provisions of Article 8 of the ECHR (right to privacy and data protection) in the context of electronic communications. The Directive is in turn transposed into UK legislation by means of the Telecommunications (Data Protection and Privacy) Regulations 1999.
[181] 8th Report from the Commission on the Implementation of the Telecommunications Regulatory Package (COM(2002) 695 final, 3rd December 2002). The second annex (Regulatory Data) to the 9th Report COM(2003)715 final, is also relevant.

> *… The retention period is set at a maximum of twelve months in the primary legislation of [Denmark, Spain, France, and Luxembourg]. [In] Belgium … twelve months is the minimum. In Spain the retention obligation applies to information society services. In Germany traffic data retention for law enforcement purposes can be imposed on operators in individual cases and requires a court order. In the United Kingdom the time periods under consideration for retention of traffic data for national security purposes vary between six and twelve months. Regarding pre-paid cards and Internet Service Providers, there is an obligation in the Netherlands to retain a limited set of traffic data for three months for the purpose of criminal investigation.*

377. Even within the UK, service providers' retention practices vary considerably. Some providers keep telephony data for a matter of months, while others are said to retain it for years.

378. Hazel Blears MP cited industry trends towards retaining less data as a reason for introducing minimum retention periods:[182]

> *I should like to revisit the reasons that have already been given for the need for the code of practice on data retention, and emphasise the critical use to which the data are being put during an investigation. Although much of this data is already kept by the industry, there is an accelerating trend in the industry either to reduce the period for which data are kept or, worse still, to stop retaining data at all. That trend is fuelled by the cost of retention and the diminishing need to keep data due to technological advances.*
>
> *I can give the Committee an example of one such technological advance: increasingly, criminals and terrorists are seeking to use pay-as-you-go mobile phones, which can be disposed of after a short time. The industry would normally keep the data on pay-as-you-go phones only during the period for which the payment subscription is made. In the past, and in other circumstances where people have had a regular long-term contract for a telephone, companies have normally kept the data for a lengthy period.*
>
> *As the business process and our use of technology changes, there is less of a case for keeping data for any significant period.*

Access to communications data

Usage

379. The total number of times that communications data has been accessed is not known because there has been no central oversight of all the different legislative routes for accessing it.

380. Access to communications data by public bodies is, however, extensive, but most access is not related to terrorism:

    a. the police service, revenue departments and intelligence services make approximately half a million requests for communications data annually. About 90

[182] Standing Committee on Delegated Legislation, 13th November 2003, col. 7.

per cent of all requests for communications data are for subscriber information (such as names and addresses).[183]

b. in the 12 months after 11 September 2001, more than 10,000 requests related to terrorist activity were made.[184]

381. Recent data is the most accessed (e.g., to determine where a rogue plumber lives), but older data can be useful when building up historical patterns of association amongst suspects.

Legal framework

382. The legal framework governing the availability of communications data to public authorities is diffuse.[185] The main principles are that a public authority can only obtain or disclose information to the extent that it has statutory or common law powers to do so. For example:

a. the police and Customs and Excise can obtain information in relation to evidence of serious offences under the Police and Criminal Evidence Act 1984;

b. authorised Department of Work and Pensions and local authority staff can gain access to certain types of communications data under the Social Security Fraud Act 2001;

c. other legislation governing access to information includes the Charities Act 1993 (used by the Charity Commission), the Criminal Justice Act 1987 (used by the Serious Fraud Office), the Environmental Protection Act 1990 (used by the Environment Agency and local authority environmental health officers), the Financial Services and Markets Act 2000 (used by the Financial Services Authority and the Department of Trade and Industry Companies Investigation Branch) and the Health and Safety at Work Act 1974 (used by the Health and Safety Executive).

383. Such powers are constrained by overarching legal frameworks, most notably the Human Rights Act 1998 and the Data Protection Act 1998.

384. The Regulation of Investigatory Powers Act 2000 (RIPA) also covers this ground. Chapter II of Part I of RIPA introduces a single human-rights-compatible statutory framework for access to communications data by public authorities. Accordingly access to communications data must be necessary for fighting crime or another defined public interest purpose[186] and the extent of access must be "proportionate" to what this access seeks to achieve. While this access framework is intended to replace and update the

---

[183] *Access to Communications Data, a consultation paper*, Home Office, March 2003, Chapter 2, paragraph 6.

[184] *On a Code of Practice for Voluntary Retention of Communications Data, a consultation paper*, Home Office, March 2003, paragraph 9.1.

[185] See Annex B of *Access to Communications Data – respecting privacy and protecting the public from crime*, Home Office consultation paper, March 2003.

[186] The purposes are: in the interests of national security; for the purpose of preventing or detecting crime or of preventing disorder; in the interests of the economic well-being of the United Kingdom (where there is a direct link with national security); in the interests of public safety; for the purpose of protecting public health; for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

earlier legislation, it does not repeal the earlier authority-specific access provisions and it is not clear what safeguards are in place to prevent them from continuing to be used.[187]

385. Chapter II of Part I of RIPA came into force after 13th November 2003 when, following consultation after the withdrawal of a June 2002 Order, Parliament agreed to the Regulation of Investigatory Powers (Communications Data) Order 2003.[188] On the face of RIPA,[189] this access framework is available to the police, revenue departments and intelligence and security services, but the list can be, and has been, extended by Order.[190]

Provisions

386. The purpose of Part 11 is to provide a legal framework within which communications service providers can retain data beyond the normal business use period for access by law enforcement, security and intelligence services. Two approaches are provided for: a voluntary code and a reserve power for the Home Secretary to require communications data to be retained.

Voluntary Code

387. Part 11 allows for the introduction of a voluntary Code of Practice which is intended to give communications service providers a clear remit to retain communications data for national security and related purposes beyond the time for which they would retain it for their own commercial purposes.[191]

Disparity of purpose

388. In March 2003 the Home Office consulted[192] publicly on such a Code. They argued that the fact that data was held by a communication service provider under the voluntary Code of Practice for national security purposes should not prevent the police or other public authorities from having access to the data for other purposes, when there was a

---

[187] Standing Committee on Delegated Legislation, debate on Draft Regulation of Investigatory Powers (Communications Data) Order 2003, 4th November 2003, Column 23: Caroline Flint (Parliamentary Under-Secretary of State, Home Office): "… On the repeal of legacy powers, we have, as I have said, a system that provides cover for organisations and is clear, and a set of checks and balances. We expect public authorities to use RIPA under the order, and we have no reason to suppose that any of them wants to use something else or to work outside it. That is welcome, because it brings transparency and the ECHR regulations with it; that is a protection for those organisations … one reason why aspects of [the legacy legislation] are still needed is that did not account for modern forms of legislation, and as we have, it is fair to say, wholesale support for the use of RIPA and the framework, there is no need for repeals."

[188] Regulation of Investigatory Powers (Communications Data) Order 2003—the Order was approved, but an an amendment to the motion was passed in the House of Lords, "[calling upon] Her Majesty's Government to lay a new draft order requiring the Interception of Communications Commissioner to inform any person who appears to have been adversely affected by any wilful or reckless failure on the part of any person exercising or undertaking any of the powers and duties conferred or imposed on him by the Regulation of Investigatory Powers Act 2000 in relation to the acquisition or disclosure of communications data, subject to national security safeguards". A further amendments was also passed "[calling upon] upon Her Majesty's Government to lay a new draft order only when a full report has been given to Parliament on the entitlement (and the conditions attaching thereto) on the part of any foreign government, body or person to require access to communications data in the United Kingdom pursuant to any legislation, agreement, treaty or convention whether national, international or in relation to the European Union and when the Government have taken note of Parliament's view on that report."

[189] Section 25(1).

[190] Regulation of Investigatory Powers (Communications Data) Order 2003.

[191] The Section 102(3) limitation to retention for national security and related purposes was a House of Lords amendment in the closing stages of the Bill.

[192] *On a code of Practice for Voluntary Retention of Communications Data*, Home Office, March 2003.

"proportionate" need. This "disparity of purpose" between retention and access seems to us to be a fundamental difficulty with the framing of these provisions. The Information Commissioner has also drawn Parliament's attention to this difficulty.

389. In September 2003 the Home Office published the results of the consultation and laid before Parliament the Orders required to introduce the voluntary Code, the access regime under the Regulation of Investigatory Powers Act 2000 and an Order to continue Part 11 beyond December 2003. The summary of the consultation responses said:

> *13. The question of the disparity between the retention and access regimes was mentioned in 25 responses. Twenty-four of those considered the matter as a problem that needed to be resolved. One respondent commented 'There is a legal view that while the retention may not in itself be unlawful, there is a significant risk that the collateral use of such retained data beyond investigations relating to national security would infringe an individual's right.'*
>
> *14. Broadly speaking the comments delivered during the consultation process encompassed the issues of legal exposure including the Human Rights implications, competitive neutrality and cost recovery. The consensus was that a voluntary approach was unable to resolve these matters and that the voluntary nature of the Code would not deliver an 'across the board' solution and clearly, issues of national security demand such a resolution.*
>
> *15. The industry indicated their view that it was necessary to ensure retention was on a firm lawful basis. The Information Commissioner indicated if there was a need for such retention, the Commissioner would prefer this to be on the basis of a statutory duty which would provide a greater degree of certainty than is possible with this voluntary arrangement.*
>
> *16. However, respondents also considered that the introduction of a mandatory regime under the Anti-terrorism, Crime and Security Act would still leave the issue of disparity unresolved and, in their view, additional legislation would be needed to resolve their concerns.*
>
> ***Conclusion***
>
> *17. The consultation paper provoked a lively debate about data retention across a broad spectrum of interested parties and reconfirmed industry's commitment to helping the government achieve its aims in the fight against terrorism.*

390. In its report on the Voluntary Code of Practice Order, the Joint Committee on Human Rights said that it was "prepared to accept the Government's view that, as a matter of policy, it should be possible to have access to any communications data which are available and are relevant to a case if those conditions [of necessity and proportionality][193] are satisfied on the facts of a particular case."

391. Nevertheless, we believe it would be beneficial both for users and subjects of the data if retention and access were based on a coherent statutory framework: the Home Office have indicated that work in the EU context may, eventually, provide the basis of such a framework.

[193] These are the conditions that Section 22 (1) and (5) of the Regulation of Investigatory Powers Act 2000 require a designated person to consider in relation to access to data under that Act. Joint Committee on Human Rights, Session 2002-3, Sixteenth Report, paragraph 25.

392. The Retention of Communications Data (Code of Practice) Order was passed on 13th November 2003.

Mandatory retention of communications data

393. The Home Secretary may issue compulsory directions[194] if he is not satisfied that the operation of the voluntary code of practice is effective. Directions may only be given if the Home Secretary is authorised to do so by affirmative order and for the purposes of safeguarding national security and the prevention and detection of crime or the prosecution of offenders which may relate directly or indirectly to national security.

394. The Government has said that it will review the operation of the voluntary code that has been introduced by means of the Retention of Communications Data (Code of Practice) Order 2003 and if (as seems to us likely) the main communications service providers do not take up the voluntary Code, it will consider issuing compulsory directions.[195]

395. The power to issue compulsory retention directions is subject to renewal every two years; it will lapse unless it is either exercised or renewed. Such a renewal was made by means of the Retention of Communications (Extension of Initial Period) Order on 13th November 2003.

Our view

396. **We can see the case in principle for requiring communications data to be retained for a minimum period (which would vary with the type of data) for a defined range of public interest purposes such as helping in the prevention and detection of terrorism and other serious crime. These provisions should, therefore, be part of mainstream legislation and not special terrorism legislation.**

397. From what we have seen, the costs of retention do not appear to be excessive.

398. However, there are obvious risks to privacy in keeping information about individuals. The existence of data creates its own demand for access to it from a wide range of bodies for a variety of reasons, mostly unrelated to national security.[196] It also creates the potential for abuse. It is, therefore, important to maintain strict limits on the Government's ability to require data to be retained and on the circumstances in which data can be accessed, and to ensure that the access rules are strictly enforced.

399. Part 11 does not provide a sound legislative basis for the retention of communications data because, no matter whether the retention requirements are implemented by a voluntary code or by mandatory order, the legality of access to that data for purposes unrelated to national security will remain contentious.

400. It is important that the consensus for retaining communications data for purposes related to national security is not undermined by demands for access to it for less important purposes.

401. **In our view the Government should accept the logic of the results of its consultation and replace Part 11 with a mainstream communications data retention regime which limits in primary legislation the longest retention period which the**

[194] Anti-terrorism, Crime and Security Act 2001, Section 104.
[195] House of Commons Standing Committee on Delegated Legislation, 13th November 2003: cols 9-10.
[196] Chapter 2 and Annex B of *Access to Communications Data*, Home Office, March 2003, discusses the range.

Government can impose to one year. This approach seems to have been adopted in several other European countries. It would permit data which is of potential use in safeguarding national security to be retained. Access to the data must, however, be subject to strict regulation, and that regulation must be properly enforced.

Maximum retention period of one year

402. The Information Commissioner's response to the Home Office consultation on the draft voluntary Code included the observations:[197]

> *… the Commissioner is yet to be convinced that there is a need for a communications service provider (CSP) to retain data routinely for the prevention of terrorism, for any longer than the data would be normally retained for its own business purposes…*
>
> *The Commissioner does though recognise that the maximum retention period of 12 months now put forward in Appendix A of the Code of Practice causes considerably less concern from a privacy point of view than some of the more extensive retention periods that have been suggested in the past.*

403. The maximum retention period is difficult to judge. Most data to which access is required is recent (e.g., current addresses or recent phone records). It has been one of the industry's complaints that no objective case has been put to them quantifying the benefits of particular retention periods (e.g., in terms of the number of crimes that would be prevented or solved). No matter what period is fixed there will always be prominent cases that fall outside it.

404. Limiting the maximum retention requirement to one year would, in our view, strike a balance. It would

    a. satisfy justifiable needs for communications data for combating terrorism and other serious crimes;

    b. be in line with the Home Office's own proposals which vary between 1 year for subscriber data and 4 days for web activity logs;

    but it would also time-limit the curtailment of the right to privacy of the individual.

Access to communications data

405. The supervisory framework for retention and access is complicated, with responsibility at present divided between the Interception (for access) and Information (for retention) Commissioners. We believe that **the whole retention and access regime, including for those access routes not governed by the Regulation of Investigatory Powers Act 2000, should be subject to unified oversight by the Information Commissioner.**

406. More generally, we recognise that **the need to retain communications data for terrorism and other serious crimes creates the potential for other use or abuse of that data. The protection provided by the Regulation of Investigatory Powers Act is a step in the right direction where it applies, but a coherent legislative framework governing both retention of, and access to, communications data seems to be the only way of providing a comprehensive solution to this issue**.

[197] http://www.informationcommissioner.gov.uk.

Data preservation

407. Where a particular suspect is already known, it would help some investigations to be able to prevent the deletion or anonymisation of communication data relating to a specified account. This is known as data preservation and has been favoured by the European Data Protection Commissioners as an alternative to data retention.

408. Data preservation is the technique used in the USA, where there are no comparable destruction or retention requirements, and where the industry structure is more complex than in the UK. A large proportion of UK emails are stored by US service providers on servers in the USA.

409. A form of data preservation has already been used in the UK. Shortly after 11th September 2001, communications service providers were asked to preserve data from the period around the attacks on the USA. The Information Commissioner was satisfied that the request was lawful. The request to preserve the September data was eventually extended until the middle of February 2002.

410. **Data preservation** would, of course, not help in cases where communications data was being used in an investigation to build up a historical pattern of association. It **is**, nevertheless, **a useful supplement to data retention, and it should, in our view, be properly provided for and regulated in the legislation.**

D.12: Part 12 – Bribery and Corruption

Provisions

411. The United Kingdom signed the OECD *Convention on Combating Bribery of Foreign Officials in International Business Transactions* in 1997. Under the Convention, signatories are required to ensure that the bribery of foreign officials is criminalised in their domestic law.

412. Part 12 made it clear that the existing common law and statutory offences of bribery and corruption were also applicable to actions by UK nationals abroad. The Government had maintained that this was already the case, but an OECD peer review group, tasked with investigating provisions in UK law in 1999, thought that the position was unclear, and recommended that the law on this point needed to be set out more explicitly for the UK to meet its obligations under the Convention.

413. A second OECD peer review group has now approved the law as revised by Part 12.

Usage

414. There have been no charges brought under Part 12 for extra-territorial corruption offences.

Our view

415. It is welcome that these measures, which have little direct bearing on terrorism, but are in themselves largely uncontroversial, are going to be repealed and replaced in their proper context, the Corruption Bill, which is currently subject to consultation.

416. The absence of convictions however calls into question the argument presented in 2001 that the inclusion of the measures in the Anti-terrorism, Crime and Security Act was justified on the grounds that they would help as part of wider counter-terrorist strategies.[198]

[198] House of Commons Debates: 21 November 2001, col. 418:
"Beverley Hughes (Minister of State, Home Office): I disagree entirely with the argument that the right hon. and learned Gentleman just made, and which the hon. Member for Woking (Mr. Malins) made in his introduction: that there is no relationship between these clauses and terrorism. Some Members on the Opposition Front Bench do not share their views either. There is obviously a relationship, in that corrupt Governments help to create the conditions that engender terrorism and we need to make it clear that the bribery of foreign officials is just as unacceptable as the bribery of United Kingdom officials."

417. It has been put to us that the low prosecution rate under Part 12 is inevitable, as it depends on complex international investigations. However, Part 12 drew on domestic provisions which have been criticised for being obscure.[199]

418. A Joint Select Committee has now had a chance to comment on a draft Bill[200] which borrowed extensively from the existing legislation in this field, primarily the Public Bodies Corrupt Practices Act 1889 and the Prevention of Corruption Act 1906, which had already been amended by this Part of the Anti-terrorism, Crime and Security Act.

419. Their report highlighted a number of difficulties with the existing measures and the approach of the Bill which rests upon them. This illustrates the importance of providing for such matters in the appropriate legislative context where they will receive consideration in sufficient depth.

420. Evidence from a representative of OECD to the Joint Select Committee emphasised concerns about the language of the Bill in relation to foreign jurisdiction, and commended the approach that other common law countries had taken in simply reproducing the language of the OECD Convention in their laws.[201]

421. **We endorse the view of the Joint Committee on the Draft Corruption Bill that a radical simplification of the bribery and corruption law in the forthcoming Corruption Bill would enhance its impact: it would serve as a better basis for prosecution, and send a clearer practical message to those professionals who are most affected by it.**

[199] In 1997 the Law Commission had recommended a new bribery statute on the grounds that existing law was "outmoded, uncertain and inconsistent," Law Commission press notice. In 2001, Transparency International expressed the view that it was unsafe "to rely on an extension of the common law offences of bribery, which are numerous, obscure and seldom used by prosecutors"; Transparency International Note, 15th November 2001.

[200] Joint Committee on the Draft Corruption Bill, Report, HL 157, HC 705, Session 2002-3.

[201] Joint Committee on the Draft Corruption Bill, Report, HL 157, HC 705, Session 2002-3, Oral evidence Q. 357-360.

D.13: Part 13 – Miscellaneous

Third pillar of the European Union

422. Section 111 allowed certain EU obligations relating to police and judicial co-operation in criminal matters to be transposed into UK legislation by secondary, rather than primary, legislation.

423. It was time-limited by Parliament and expired in July 2002. We note that most of the EU provisions for which it was intended to use Section 111 had not been agreed before it expired. Some have subsequently been enacted by primary legislation, in principle allowing for more thorough Parliamentary scrutiny than they would otherwise have enjoyed.

424. The case for using secondary legislation in police and judicial co-operation ("third pillar") matters on the basis that it would avoid legislative overload is weaker than in the "first pillar" (for example, single market) context because:

    a. issues of liberty and accountability tend to arise in legislation on policing and the judicial process to a greater extent;

    b. unlike, for example, the single market programme, the volume of "third pillar" obligations is not high;

    c. not all such obligations require legislation:

        i. UK legislation is often fully or wholly in compliance with them;

        ii. Some obligations require administrative and not legislative action.

    d. implementation deadlines have not been unmanageably tight;

    e. there is a greater frequency of primary legislation suitable for enacting third pillar legislation (e.g., criminal justice bills).

Dangerous Substances

425. Sections 113-5 relate to the use or threatened use of "noxious substances". Section 113 creates a new offence of using or threatening to use a noxious substance in a way that would involve serious violence or damage to influence the government or intimidate the public. It is designed to cover those individuals who seek to cause havoc by, for example, sending anthrax through the post, damaging fields or polluting water supplies.

426. The scope of the offence includes someone acting or threatening to act in the UK even if the subject of the action or threatened action is outside the UK at the time (for example, sending a parcel containing anthrax from the UK to someone in France with the intention of causing harm there).

427. Section 114 creates a new offence of hoaxing which involves noxious substances or things. The essence of the hoax is that the substance used is not the substance it seems to be. It brings legislation into line with bomb hoaxes as a terrorist weapon. For example,

scattering white powder in a public place or spraying water droplets around in an Underground Train could fall within the scope of the new offence.

428. Three incidents where individuals have been held or charged with offences involving hoax noxious substances under Section 114 have been reported to us.

429. These seem to us to be unexceptionable provisions. We believe that the concerns which were expressed at the time of the Bill, that the provisions could be used to stifle *legitimate* protest through (e.g.) the disruption of genetically modified crop experiments by the use of destructive chemicals, are unjustified.

Intelligence Services Act 1994

430. Section 116 relaxed certain authorisation procedures, bringing arrangements for the oversight of certain operations by GCHQ into line with those created for the Secret Intelligence Service under the Intelligence Services Act 1994. We are satisfied that these provisions raise no new points of principle.

Terrorism Act 2000: withholding information

431. Section 117 amends the Terrorism Act, making it a criminal offence (subject to a defence of reasonable excuse) to fail to disclose information about acts of terrorism.

432. It reinstates a similar offence which had been included in Section 18 of the Prevention of Terrorism Act 1989, but was excluded from the Terrorism Act in response to a recommendation by Lord Lloyd. His recommendation reflected a number of difficulties with the offence: it puts relatives of terrorists into a dilemma and potentially criminalises lawyers for withholding information which would normally be regarded as privileged. Its practical impact in increasing the level of information supplied to the police had also been regarded as doubtful.[202]

433. In principle, it would be preferable if such an offence did not exist. However, we note that the offence has had some use since 2001, with charges brought against three individuals in relation to serious terrorism cases. A similar offence is available in Germany.[203]

434. **It is preferable for prosecution to take place on the grounds of direct involvement in terrorism where possible, but we understand that use of the offence of withholding information may be the only way forward in some serious cases. We invite Lord Carlile to keep the operation of this section under particularly careful review**.

Section 119: Advance Passenger Information

435. This Section is discussed above, at page 80, under Part 9 ("Aviation Security").

[202] Views on the provision were summarised by Lord Lloyd, *Inquiry into Legislation against Terrorism,* pages 93-4.
[203] Article 138, paragraph 2, Criminal Code.

D.14: Part 14 – Supplemental

436. Part 14 covers such matters as review, commencement, and amendment of the Act.

Consequential and Supplementary Provisions

437. Section 124 gives the Government extensive powers to amend or supplement the Act and other legislation by statutory instrument. It remains unused.

Our view

438. It is accepted that it is appropriate for some Acts of Parliament to include provision for so-called "Henry VIII" powers,[204] which permit the Government to make technical amendments to Acts of Parliament through subordinate legislation. Such powers are always controversial, but they have been included in Acts where the legislative framework is complex, and where it is argued that it would be burdensome for Parliament to debate minor changes that follow strictly from the terms of the primary legislation which it has already approved.

439. The Home Office memorandum on the Bill submitted to the Delegated Powers Select Committee in 2001 explained the clause as follows:

> *[Section 124] confers an admittedly wide power on Ministers of the Crown… to make orders containing provisions which are consequential or supplementary on provisions of the Bill. Under subsection (2)(a) such an order may apply (with or without modifications), amend, repeal or revoke any provision of, or made under, an Act which is enacted before the Bill or in the same Session as the Bill…*
>
> *Unsurprisingly, in view of these powers any such order is subject to the affirmative resolution procedure.*
>
> *As the Committee is aware, the Bill has been drafted as a response to the possible threat to national security following the horrifying attacks in the United States of America on 11 September. Whilst it is hoped that the consequential amendments that need to be made have been identified, it would be unsafe to assume that this is necessarily the case. Accordingly, some safety measure such as is provided by this clause seems desirable.*[205]

440. In fact, the powers created by section 124 are amongst the broadest of their kind in that:

    a. they provide for "supplemental", as well as merely "consequential" amendments;

[204] The name derives from the Statute of Proclamations 1539, which conferred on King Henry VIII the power to make proclamations which would have the force of ordinary legislation.
[205] The Memorandum is appended to House of Lords Select Committee on Delegated Powers and Regulatory Reform, Sixth Report, 11 December 2001.

b. they are subject only to negative resolution procedure,[206] contrary to the explanation given in the Home Office memorandum, and;

c. they include a power to amend legislation passed before the 2001 Act.

441. This combination is not totally unprecedented,[207] but it is inappropriate and unwelcome in an Act where so many provisions were known to be controversial, raising a number of civil liberties issues.

442. **The powers of amendment set out in Section 124 are particularly unwelcome in emergency legislation of this kind, and they should be repealed.**

[206] That is, they do not need to be approved by an affirmative vote in Parliament at all. With certain very limited exceptions, delegated legislation subject to the affirmative or the negative procedure may not be amended by either House of Parliament. Instruments exercising delegated powers are affirmed, or made the subject of a "prayer" (a motion to annul) as a whole. In the House of Commons, the Government cannot be forced to find time for a debate on a motion to annul or to revoke an instrument subject to negative resolution, either on the floor of the House or in Committee. If such an instrument were to be referred to a Standing Committee, the motion for debate would be "that the Committee has considered the instrument": even if such a motion were defeated in Committee, there would be no legal or procedural consequences, and the Government would not be obliged to put the substantive motion to the House.
The House of Lords Committee on Delegated Powers takes the view that all such instruments should be subject to affirmative resolution procedure: Session 2002-3, 3rd Report.

[207] See for instance Section 426 of the Financial Services and Markets Act 2000.

E: Annexes

E.1: The Review

443. This Review was given no formal terms of reference. However, the material below sets out the formal basis of the Committee's work.

Sections 122 and 123 of the Act

Sections 122 and 123 of the Act set out the remit for this Review:

122 Review of Act

(1) The Secretary of State shall appoint a committee to conduct a review of this Act.

(2) He must seek to secure that at any time there are not fewer than seven members of the committee.

(3) A person may be a member of the committee only if he is a member of the Privy Council.

(4) The committee shall complete the review and send a report to the Secretary of State not later than the end of two years beginning with the day on which this Act is passed.

(5) The Secretary of State shall lay a copy of the report before Parliament as soon as is reasonably practicable.

(6) The Secretary of State may make payments to persons appointed as members of the committee.

123 Effect of report

(1) A report under section 122(4) may specify any provision of this Act as a provision to which this section applies.

(2) Subject to subsection (3), any provision specified under subsection (1) ceases to have effect at the end of the period of 6 months beginning with the day on which the report is laid before Parliament under section 122(5).

(3) Subsection (2) does not apply if before the end of that period a motion has been made in each House of Parliament considering the report.

Parliamentary debate

444. These sections were added to the Bill near the end of its passage through Parliament. They were debated on 10th, 12th and 13th December 2001:

House of Lords Hansard: 10th December 2001, Cols 1203-1204:

> ***Lord Rooker**: We have included a review of the asylum and detention powers after 15 months, then annually thereafter. Any part of the Bill that amends the Terrorism Act 2000 will… be reviewed annually as part of that legislation's requirements where a report on the Act's operation must be laid before Parliament at least once every 12 months. The noble Lord, Lord Carlile of Berriew, has been appointed to undertake those reviews.*
>
> *We are not convinced of the need for more sunset clauses covering parts of the Bill or the whole measure. However, the speed with which this legislation is being passed must be recognised by the Government. […]*
>
> *I am proposing a new clause which will sit somewhere in the latter part of the Bill, probably Part 14, but before Clause 122, as it is now. There will be a statutory review of the Act in addition to all the other "sunset" clauses and reviews which already appear on the face of the Bill. It is a small, new clause. The Secretary of State shall appoint a committee to conduct a review of the Act. He will seek to secure that at any time there will be no fewer than seven members of the committee. It may be more, but seven is the minimum. Every person on that committee will be there only if they are a member of the Privy Council.*
>
> *The committee will complete a review of the operation of the Act with full access to all the information including that from the security services and so forth. A report will be sent to the Secretary of State not later than two years after the Act is passed. The Secretary of State will be bound on the face of the Act to lay a copy of that report before Parliament as soon as reasonably practical. We shall then say from the Dispatch Box in this House and the other place that we shall guarantee that the business managers will arrange dates and days in both Houses when the report will be debated. It will be detailed.*
>
> *It will be no use anyone saying, "Will you accept the recommendations?" That cannot be said at this point. If such a report is laid with suggestions for amendments to the Act, if they are not accepted the Ministers concerned will need to have very good reasons for not doing so, bearing in mind that people will have had access to all the relevant information and had a good review of the operation of the Act over the period of two years. It will then be for both Houses to make a judgment on the content of the recommendations. […]*

House of Commons Hansard: 12th December 2001, cols 952-953

> ***Mr. Blunkett**: On sunset clauses, the Government have taken several measures in response to the Select Committee on Home Affairs and to the wishes of individual Members and to debates held earlier on part 4. Those measures include a sunset clause after five years, review after a year and other provisions that reflect the will of the House.*

I want to make it clear—so that there is no doubt in the other place—that we strongly resist any further move on sunset clauses. We shall not allow the Bill to be dismembered by the indiscriminate application of sunset clauses to different parts of it. Having voted on those matters when the Bill was before the Commons for the first time, and after having those provisions overturned by the House of Lords, it is clear that we have listened and responded to concerns on the main clauses of the Bill. It is not possible for the Government to decide that a Bill should be completely taken apart—nor has that been true for any other measure—with different timings for individual provisions; and that proceedings should be repeated and the measure brought back to the House.

***Mr. Hogg**: The right hon. Gentleman will, of course, speak to Government amendment (a), which proposes that the review should be undertaken by*

"not fewer than seven members of the"

Privy Council. Would he be so good as to tell us by what criteria he will select those members of the Privy Council?

Why should we assume that they will not be carefully picked nominees? Would he further give an undertaking that the report will not merely be laid before the House

"as soon as is reasonably practicable",

but be debated by the House, preferably on a free vote?

***Mr. Blunkett**: […] Of course, we shall consult the Opposition parties on the committee of review's make up, so the House should agree to the Government amendment in lieu of the Lords amendment to provide a review committee, which would report within two years. That report would be laid before the House of Commons, and both Houses would hold a full debate on it. I am prepared tomorrow to consider the suggestions that the Opposition parties are putting to me to strengthen that proposal. Clearly, the review committee's recommendations on individual parts of the Bill would be taken forward by the Government. […]*

***Norman Baker**: I pay tribute to the Home Secretary for the constructive way in which he has approached this matter and others. I welcome some of his positive responses—"concessions" sounds too dismissive—and the way in which he has changed the wording of the Bill accordingly. However, we are not convinced that enough progress has been made on sunset clauses, and I shall be asking my colleagues to agree with the Lords, not the Government, when we come to vote in 17 minutes or so.*

The Home Secretary mentioned a review, and it would be helpful if tomorrow some flesh were put on the bones of that. If the review would result in a sunset clause of a different nature, we would be willing to hear about it, as, no doubt, would the Conservatives. If, however, the intention is simply to tart about with the panel of Privy Councillors that he has suggested, that will not be enough.

[…] given the nature of the Bill, it is impossible to say that it should be passed without a proper review being established. With due respect to the Home Secretary's proposals, that body of Privy Councillors does not constitute a proper review. It is a body comprising the great and the good who will consider the legislation and may comment on it, but in no way is their judgment to be binding on the Government. When Lord Rooker was asked whether the recommendations of the review would be accepted, he replied:

"That cannot be said at this point."—[Official Report, House of Lords, 10 December 2001; Vol. 629, c. 1204.]

In other words, he gave no undertaking that the comments made by that body of Privy Councillors would be accepted by the Government. […]

***Mr. Blunkett**: Let me make it clear that Lord Rooker could not give that assurance because we had not agreed it at that time. However, I have just given it, and if I say from the Dispatch Box that that is what we are going to do, that is what we are going to do. […]*

In response to those who are sceptical and believe that we are packing the measure or are being elusive, if we were prepared to take seriously what was said by a committee that undertook a review and could take security evidence but, after debate in both Houses, we were not prepared to respond to it, we would be making a rod for our own backs. Making sure that what we say and do is credible is a matter of both will and necessity; there should be trust that that will happen.

House of Commons Hansard: 13th December 2001, col.1110:

***Mr. Blunkett:** […] It has been suggested, particularly by the Liberal Democrats, that every part of the Bill should have to be revisited and rerun through Parliament. That, of course, would be at the expense of other measures proposed by, among others, the Liberal Democrats. We believe that, after sensitive deliberation on the matters that are of most concern and after agreement had been reached, it would be right to seek a return only if it was considered that remaining parts not given sunset clauses had prompted concern. We therefore proposed a review by a Privy Council committee, which would report to the two Houses within two years, and recommended that the terms of its report should be debated by the House of Commons.*

There appears to have been doubt about whether the commitments given by the Government would result in full deliberation in relation to any concerns expressed by the committee. Our amendment[208], while declining to provide sunset clauses in regard to every part of the Bill and therefore to rerun those parts, does ensure that the review can highlight areas in which the committee believes there is cause for concern in terms of implementation, and therefore that we would guarantee a sunset clause of six months on any such items should the two Houses not have an opportunity to deliberate fully.

[208] That is, the clause which became Section 123.

> *We consider this a sensible amendment, which should reassure everyone that the Government will have to provide a debate and will have to reach conclusions on the issues highlighted by the review committee.*

Parliamentary Questions

445. The following written PQ (House of Commons Hansard, 24th May 2002, col. 702W) is also relevant:

> ***Review Committee (Anti-Terrorism Legislation)***
>
> ***Mr. McNamara:*** *To ask the Secretary of State for the Home Department what the terms of reference are for the Review Committee of Anti-terrorism, Crime and Security Act 2001; to whom it reports; what its annual budget and proposed staff are in its first year; what its sphere of competence is; what immunities its members enjoy; and what powers the body has (a) to compel witnesses, (b) to seize documents, (c) to demand disclosure, (d) to initiate its own inquiries, (e) to publish its reports and address the media by other means, (f) to create its own sub-committees and (g) to consider complaints by individuals and groups.[54542]*
>
> ***Mr. Blunkett:*** *Section 122 of the Anti-terrorism, Crime and Security Act 2001 sets out the Parliamentary requirement for a Committee to undertake a review of the Act. The Committee will report to me when they have completed their work. The Act requires them to deliver this by 14 December 2003.*
>
> *There are no powers for the Committee to compel individuals or organisations to provide information. But the Government would expect and encourage those individuals and organisations who are approached to co-operate fully with any request made to them by the Committee. All questions of procedure and staffing are for the Committee themselves to decide. While no specific budget has been set, the necessary funds will be made available to the Committee to enable them to do their work.*

E.2: Contributors

446. In carrying out its work, Committee Members took oral evidence from:

- Association of Chief Police Officers
- British Airports Authority plc
- British Transport Police
- Jean-Louis Bruguière, Premier Vice-Président chargé de l'instruction, Tribunal du Grand Instance, Paris
- Campaign Against Criminalising Communities (CAMPACC): Stephanie Harrison, Ghayasuddin Siddiqui, Les Levidow and Dabinderjit Singh OBE
- Canadian Security Intelligence Review Committee
- Lord Carlile of Berriew QC
- Communications Service Providers: Howard Lamb (Energis), Martin Hoskins (T-Mobile), Tony Smith (BT), Emma Ascroft (C&W) and Clive Feather (Thus)
- HM Customs and Excise officials
- Forum Against Islamophobia and Racism (FAIR): Shareefa Choudhury, Layli Uddin, Muddassar Arani (Arani & Co), Sadiq Khan (Christian Khan Solicitors) and Imran Khan (Imran Khan & Partners)
- Professor Conor Gearty (London School of Economics)
- The Heritage Foundation, Washington DC: Paul Rosenzweig and Mick Scardaville
- Home Office officials
- Inland Revenue Special Compliance Office
- Kent Constabulary
- The Law Society: Peter Williamson (Vice President) and Vicki Chapman.
- Liberty: John Wadham (Director), Shami Chakrabarti and Joanne Sawyer
- Metropolitan Police
- Metropolitan Police Special Branch
- Ministry of Defence officials
- Ministry of Defence Police
- National Criminal Intelligence Service

- Gareth Peirce (Birnberg Peirce and Partners)
- Secret Intelligence Service officials
- Security Service officials
- Special Advocates
- Special Immigration Appeals Commission judges
- Department of Trade and Industry officials
- Department for Transport officials
- Professor Paul Wilkinson (University of St Andrews)
- US administration officials

447. The Committee has also received helpful submissions from

- Amnesty International UK
- David Bickford
- Ian Burnett QC
- Sir Adrian Fulford
- Simon McKay (Simon McKay Solicitors)
- Professor Clive Walker (University of Leeds)

448. In addition, the Committee's secretariat benefited from discussions with, and advice from, a number of people and organisations, including:

- Professor John Bell QC (Cambridge University)
- Sir Louis Blom Cooper QC
- Representative Howard Coble (Chairman of House of Representatives Judiciary Subcommittee for Crime, Terrorism and Homeland Security)
- Commissioner Ian Davis, Australian Law Reform Commission
- Viet D. Dinh, U.S. Assistant Attorney General
- Fabrice Dubest
- Ben Emmerson QC
- Graham Hooper (Barclays Bank)
- Gregory Nojeim (American Civil Liberties Union)
- Heritage Foundation: Todd Gaziano, Edwin Meese, Paul Rosenzweig, and Larry M. Wortzel

- Leicestershire Constabulary
- Ken Macdonald QC
- Hodge Malek QC
- Gabor Rona (International Committee of the Red Cross)
- Philip Sales
- Sussex Constabulary
- Jeremy Thorp (British Bankers' Association)
- Bob Upton (Lloyds TSB Bank)
- Senior District Judge Tim Workman
- Parliamentary Clerks
- House of Commons Library Clerks
- Parliamentary Office of Science and Technology staff
- Canadian Federal Government officials
- US administration officials
- Officials from: Home Office, Foreign and Commonwealth Office, Department of Trade and Industry, HM Treasury, Inland Revenue, Department for Transport, Department for the Environment, Food and Rural Affairs, Ministry of Defence, Cabinet Office, Charity Commission and Financial Services Authority

449. The Committee and its secretariat have also benefited from the assistance of:

- Sir Anthony Hammond QC
- Intelligence and Security Committee secretariat
- Special Immigration Appeals Commission staff
- Andy Wood and Ian Mitchell

E.3: The Review Committee

Members

450. The members of the Review Committee are:

- The Rt. Hon Lord Newton of Braintree (Chairman)
  - Life peer since 1997
  - Lord President of the Council and Leader of the House of Commons 1992-97
  - Secretary of State for Social Security 1989-92
  - Chancellor of the Duchy of Lancaster and Minister for Industry 1988-9
  - Minister for Health 1986-88
  - Social Security Minister 1982-86
  - Assistant Government Whip 1979-82
  - MP for Braintree, Essex, 1974-97 (Conservative)

- The Rt. Hon Alan Beith, MP (Deputy Chairman)
  - MP for Berwick Upon Tweed (Liberal Democrat)
  - Chairman of the Constitutional Affairs Select Committee since 2003
  - Spokesman for Home and Legal Affairs 1997-99
  - Spokesman for Police, Prison and Security Matters 1995-97
  - Deputy Leader of the Liberal Democrats (1992-2003)
  - Member of the Intelligence and Security Committee (since 1995)

- The Rt. Hon The Lord Browne-Wilkinson
  - Lord of Appeal in Ordinary (since 1991)
  - Senior Law Lord 1998-2000
  - Created life Baron in 1991
  - Lord Justice of Appeal 1983-85
  - Judge of the High Court, Chancery Division 1977-83
  - Created a QC in 1972

- The Rt. Hon Terry Davis, MP
  - MP for Birmingham Hodge Hill (Labour)
  - Leader of the Socialist group in Council of Europe Assembly since January 2002
  - Vice-President of Council of Europe Assembly 1998-2002
  - Leader of the UK delegation to the Council of Europe Assembly 1997-2002
  - Member of the UK delegation to the Council of Europe Assembly 1992-
  - Leader of the UK delegation to the OSCE Assembly July 2002-
  - Member of the UK delegation to the OSCE Assembly 1997-
  - Member of the Advisory Council on Public Records 1989-94
  - Member of the Public Accounts Committee 1987-94
  - Opposition Spokesman: Trade & Industry 1986-87
  - Opposition Spokesman: Treasury & Economic Affairs 1983-86
  - Opposition Spokesman: Health and Social Services 1980-83

- The Rt. Hon Baroness Hayman
  - Chairman, Cancer Research UK
  - Minister of State, MAFF 1999-2001
  - Parliamentary Under Secretary of State, Department of Health 1998-99
  - Parliamentary Under-Secretary of State: DETR 1997-98
  - Opposition Front Bench Spokesman on Health, 1996-7
  - Created a life Peer in 1996
  - MP for Welwyn and Hatfield, 1974-79 (Labour)

- The Rt. Hon Lord Holme of Cheltenham
  - Liberal Democrat Parliamentary Spokesman on Northern Ireland 1990-1999
  - Chairman of Hansard Society for Parliamentary Government 2001-
  - Chairman Broadcasting Standards Commission 1999-2000
  - Chancellor, University of Greenwich 1999-
  - Director Rio Tinto, and then Special Adviser to the Chairman 1994-
  - Adviser to NTL, the cable company, 2001-
  - Created Life Peer 1990
  - Received CBE 1983

- The Rt. Hon Sir Brian Mawhinney, MP
  - MP for North West Cambridgeshire (Conservative)
  - Shadow Home Secretary 1997-98
  - Cabinet Minister without Portfolio, 1995-7
  - Chairman of the Conservative Party 1995-97
  - Secretary of State for Transport 1994-95
  - Minister of State, Department of Health 1992-94
  - Minister of State, Northern Ireland Office 1990-92
  - Parliamentary Under-Secretary of State, Northern Ireland Office 1986-90

- The Rt. Hon Joyce Quin, MP
  - MP for Gateshead East and Washington West (Labour)
  - Member of the Intelligence and Security Committee (since 2001)
  - Minister of State and Deputy Minister, Ministry of Agriculture, Fisheries and Food 1999-2001
  - Minister of state, Foreign and Commonwealth Office 1998-99
  - Minister of State, Home Office 1997-98
  - Opposition Front Bench Spokesman on Europe 1993-97
  - Opposition Front Bench Spokesperson on Employment 1992-93
  - Opposition Spokesperson on Trade and Industry 1989-92

- The Rt. Hon Dr Chris Smith, MP
  - MP for Islington South & Finsbury (Labour)
  - Director, Clore Cultural Leadership Programme
  - Visiting Professor at the London Institute
  - Senior Adviser to The Walt Disney Company Ltd
  - Chairman of Classic FM Consumer Panel
  - Chairman of Wordsworth Trust
  - Member of Wicks Committee on Standards in Public Life
  - Member of Board of Royal National Theatre
  - Secretary of State for Culture, Media and Sport 1997-2001
  - Chairman of the Millennium Commission 1997-2001
  - Shadow Secretary of State for Health 1996-97
  - Shadow Secretary of State for Social Security 1995-96
  - Shadow Secretary of State for National Heritage 1994-95
  - Shadow Secretary of State for Environmental Protection 1992-94
  - Shadow Treasury Minister 1987-92

E.4: Bibliography

451. The Review has drawn extensively on Select Committee Reports and House of Commons library research papers.

452. The following sources were also used in preparing this Report:

- Alexander, Y., and Brenner, E.H., (eds) *Terrorism and the Law* (Transnational Publishers, New York, 2001)
- Alexander, Y., and Brenner, E.H., (eds) *The United Kingdom's Legal Responses to Terrorism* (Cavendish Publishing Ltd, London, 2003)
- All Party Internet Group (APIG), *Communications Data: Report of an Inquiry by the All Party Internet Group* (APIG, London, 2003)
- The Rt Hon Lord Justice Auld, *Review of the Criminal Courts of England and Wales* (The Stationery Office, London, 2001)
- Barak, A., *A judge on judging: the role of a Supreme Court in a democracy*, Harvard Law Review, Volume 116, Part 1.
- Burke, J., *Al-Qaeda – Casting a Shadow of Terror* (I.B.Tauris & Co Ltd, London, 2003)
- Lord Carlile of Berriew Q.C., *Report on the Operation in 2001 of the Terrorism Act 2000* (http://www.homeoffice.gov.uk/docs/tact_report.pdf)
- Lord Carlile of Berriew Q.C., *Report on the Operation in 2001 of Part VII of the Terrorism Act 2000* (http://www.homeoffice.gov.uk/docs/carlirep.pdf)
- Lord Carlile of Berriew Q.C., *Section 28 Review on Part IV of the Anti-terrorism, Crime and Security Act 2001* (http://www.homeoffice.gov.uk/docs/crime_and_security_act.pdf)
- Clayton, R., and Tomlinson, H., *The Law of Human Rights – Volumes 1 & 2* (Oxford University Press, New York, 2000)
- Dershowitz, A.M., *Why Terrorism Works – Understanding the Threat, Responding to the Challenge* (Yale University Press, New Haven, 2002)
- Electronic Privacy Information Center (EPIC) in association with Privacy International, *Privacy and Human Rights – An International Survey of Privacy Laws and Developments* (EPIC, USA, 2002)
- Gardiner Report, *Report of a Committee to consider, in the context of civil liberties and human rights, measures to deal with terrorism in Northern Ireland* (Cmnd.5847, HMSO London, 1975)

- Gearty, C.A., and Kimbell, J.A., *Terrorism and the Rule of Law – A Report on the Laws relating to Political Violence in Great Britain and Northern Ireland* (The Civil Liberties Research Unit, London, 1995)
- Greer, S.C., Supergrasses*: A Study of Anti-terrorist Law Enforcement in Northern Ireland* (Clarendon Press, Oxford, 1995)
- Laqueur, W., *The New Terrorism – Fanaticism and the Arms of Mass Destruction* (Phoenix Press, London, 2001)
- The Law Society., *Underpinning Security, Safeguarding Liberty – A Memorandum to the Home Affairs Select Committee on the Anti-terrorism, Crime and Security Act 2001* (The Law Society, London, 2002)
- van Leeuwen, M., (ed) *Confronting Terrorism – European Experiences, Threat Perceptions and Policies* (Kluwer Law International, Netherlands, 2003)
- The Rt Hon Lord Lloyd Of Berwick, *Inquiry into Legislation against Terrorism – Volumes 1 & 2 (*Cm.3420, The Stationary Office, London, 1996)
- Markesinis, B., (eds) *The Gradual Convergence – Foreign Ideas, Foreign Influences, and English Law on the Eve of the 21st Century* (Oxford University Press, New York, 1994)
- Michaels, C.W., *No Greater Threat: America After September 11, and the Rise of a National Security State* (Algora Publishing, New York, 2002)
- Napoleoni, L., *Modern Jihad – Tracing the Dollars Behind the Terror Networ*ks (Pluto Press, London, 2003)
- Reinares, F., (ed) *European Democracies Against Terrorism – Governmental Policies and Intergovernmental Cooperation* (Ashgate Publishing Ltd, Aldershot UK, 2000)
- *Royal Commission on Criminal Justice Report* (Cm.2263, HMSO London, 1993)
- Schneier, B., *Beyond Fear – Thinking Sensibly about Security in an Uncertain World* (Copernicus Books, New York, 2003)
- Sterba, J.P., (ed) *Terrorism and International Justice* (Oxford University Press, New York, 2003)
- Walker, C., *Blackstone's Guide to the Anti-terrorism Legislation* (Oxford University Press, New York, 2002)
- Walker, C., *The Prevention of Terrorism in British Law* (Manchester University Press, Manchester, 1992)
- Wilkinson, P., and Jenkins, B.M., (eds) *Aviation Terrorism and Security* (Frank Cass Publishers, London, 1999)
- Wilkinson, P., *Terrorism versus Democracy: the Liberal State Response* (Frank Cass Publishers, London, 2000).

E.5: European Council Framework Decision

453. The following is an extract from the European Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA).

Article 1

Terrorist offences and fundamental rights and principles

1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:

- seriously intimidating a population, or

- unduly compelling a Government or international organisation to perform or abstain from performing any act, or

- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation, shall be deemed to be terrorist offences:

(a) attacks upon a person's life which may cause death;

(b) attacks upon the physical integrity of a person;

(c) kidnapping or hostage taking;

(d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;

(e) seizure of aircraft, ships or other means of public or goods transport;

(f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;

(g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;

(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;

(i) threatening to commit any of the acts listed in (a) to (h).

This Framework Decision shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.

Article 2

Offences relating to a terrorist group

1. For the purposes of this Framework Decision, "terrorist group" shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

2. Each Member State shall take the necessary measures to ensure that the following intentional acts are punishable:

(a) directing a terrorist group;

(b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

Article 3

Offences linked to terrorist activities

Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following acts:

(a) aggravated theft with a view to committing one of the acts listed in Article 1(1);

(b) extortion with a view to the perpetration of one of the acts listed in Article 1(1);

(c) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).

Article 4

Inciting, aiding or abetting, and attempting

1. Each Member State shall take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.

2. Each Member State shall take the necessary measures to ensure that attempting to commit an offence referred to in Article 1(1) and Article 3, with the exception of possession as provided for in Article 1(1)(f) and the offence referred to in Article 1(1)(i), is made punishable.

Article 5

Penalties

1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 1 to 4 are punishable by effective, proportionate and dissuasive criminal penalties, which may entail extradition.

2. Each Member State shall take the necessary measures to ensure that the terrorist offences referred to in Article 1(1) and offences referred to in Article 4, inasmuch as they relate to terrorist offences, are punishable by custodial sentences heavier than those imposable under national law for such offences in the absence of the special intent required pursuant to Article 1(1), save where the sentences imposable are already the maximum possible sentences under national law.

3. Each Member State shall take the necessary measures to ensure that offences listed in Article 2 are punishable by custodial sentences, with a maximum sentence of not less than fifteen years for the offence referred to in Article 2(2)(a), and for the offences listed in Article 2(2)(b) a maximum sentence of not less than eight years. In so far as the offence referred to in Article 2(2)(a) refers only to the act in Article 1(1)(i), the maximum sentence shall not be less than eight years.

Article 6

Particular circumstances

Each Member State may take the necessary measures to ensure that the penalties referred to in Article 5 may be reduced if the offender:

(a) renounces terrorist activity, and

(b) provides the administrative or judicial authorities with information which they would not otherwise have been able to obtain, helping them to:

(i) prevent or mitigate the effects of the offence;

(ii) identify or bring to justice the other offenders;

(iii) find evidence; or

(iv) prevent further offences referred to in Articles 1 to 4.

———