HOUSE OF LORDS

European Union Committee

5th Report of Session 2004-05

After Madrid: the EU's response to terrorism

Report with Evidence

Ordered to be printed 22 February and published 8 March 2005

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£22.00

HL Paper 53

The European Union Committee

The European Union Committee is appointed by the House of Lords "to consider European Union documents and other matters relating to the European Union". The Committee has seven Sub-Committees which are:
Economic and Financial Affairs, and International Trade (Sub-Committee A)
Internal Market (Sub-Committee B)
Foreign Affairs, Defence and Development Policy (Sub-Committee C)
Agriculture and Environment (Sub-Committee D)
Law and Institutions (Sub-Committee E)
Home Affairs (Sub-Committee F)
Social and Consumer Affairs (Sub-Committee G)

Our Membership

The Members of the European Union Committee are:

Lord Blackwell
Lord Bowness
Lord Dubs
Lord Geddes
Lord Grenfell (Chairman)
Lord Hannay of Chiswick
Lord Harrison
Baroness Maddock
Lord Marlesford
Lord Neill of Bladen
Lord Radice
Lord Renton of Mount Harry
Lord Scott of Foscote
Lord Shutt of Greetland
Baroness Thomas of Walliswood
Lord Tomlinson
Lord Woolmer of Leeds
Lord Wright of Richmond

Information about the Committee

The reports and evidence of the Committee are published by and available from The Stationery Office. For information freely available on the web, our homepage is:

http://www.parliament.uk/parliamentary_committees/lords_eu_select_committee.cfm

There you will find many of our publications, along with press notices, details of membership and forthcoming meetings, and other information about the ongoing work of the Committee and its Sub-Committees, each of which has its own homepage.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at http://www.parliament.uk/about_lords/about_lords.cfm

Contacts for the European Union Committee

Contact details for individual Sub-Committees are given on the website.

General correspondence should be addressed to the Clerk of the European Union Committee, Committee Office, House of Lords, London, SW1A OPW
The telephone number for general enquiries is 020 7219 5791.
The Committee's email address is euclords@parliament.uk

CONTENTS

ORAL EVIDENCE

1 Now Sir David Veness

WRITTEN EVIDENCE

NOTE: Pages of the report are numbered in bold type; pages of evidence are numbered in ordinary type. References in the text of the report are as follows:

(Q) refers to a question in oral evidence
(p) refers to a page of written evidence

ABSTRACT

International terrorism is a major scourge of modern society. Action must be mobilised against it at every appropriate level.

The EU has a role to play but it must remain a co-ordinating one in support of the Member States, which have the primary responsibility for combating terrorism. Given the range of interests involved, effective co-ordination—and the work of the EU Counter-terrorism Co-ordinator—are crucial. The present proliferation of EU groups and agencies needs to be reduced and streamlined.

Terrorism is a global phenomenon and the EU must engage with international agencies, especially Interpol, in combating it.

Accurate and timely information and intelligence are crucial to forestalling terrorist attacks and identifying the perpetrators. The EU provides a forum for more extensive exchange of information between Member States and this opportunity must be fully exploited. Such exchange of information must be subject to effective data protection safeguards. A uniform data protection regime for the Third Pillar would not only provide better data protection but would also facilitate the exchange of information.

After Madrid: the EU's response to terrorism

CHAPTER 1: INTRODUCTION

1. The growth of international terrorism has been one of the most malign developments of recent years. It poses a threat not only to the lives and wellbeing of the citizens of countries targeted by the terrorists but also—as the terrorists no doubt intend—to the very foundations of our democratic institutions. Terrorism impacts on everyone's lives, even if they are not a target or have not experienced a terrorist attack themselves. The increasing security measures that governments have judged it necessary to put in place are a constant reminder of the threat; and the apparent randomness of terrorist attacks and the increasingly prevalent phenomenon of the suicide terrorist inevitably add to the public's fear and the difficulties of countering it. Against that background it is entirely right that the European Union (EU) should have been examining as a matter of urgency what additional action at EU level is necessary to supplement and, where appropriate, co-ordinate the efforts of the Member States, which retain—and must retain—the primary responsibility for protecting their citizens.

2. Following the Madrid bombings on 11 March 2004 the European Council issued a Declaration on Combating Terrorism,[1] which identified a range of measures to be put in place. In response to elements of that Declaration the Commission presented proposals to enhance the exchange of information between law enforcement authorities on the basis of a principle of "equivalent access" by law enforcement authorities. Around the same time the Swedish Government tabled in parallel a draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities, to give police authorities in one Member State access to information and intelligence held by authorities in other Member States under conditions no stricter than those applicable at national level.[2] In October 2004 the Commission published four further Communications on other aspects of the Declaration.[3] These documents are in large part concerned with aspects of civil protection and contingency planning that go beyond the scope of this report, but we have taken account of those aspects that are relevant to our inquiry, particularly the proposals on terrorist financing, which include consideration of the case for giving law enforcement authorities access to financial databases.

3. We describe the proposals on information exchange in more detail in Chapter 2 of this Report and discuss the issues arising from them in

---

1 SN 86/1/04 REV 1.

2 Document nos. 10215/04; 10215/04 ADD 1.

3 Communications from the Commission to the Council and the European Parliament on: Prevention, preparedness and response to terrorist attacks (Document 13978/04); Critical Infrastructure Protection in the fight against terrorism (13979/04); Preparedness and consequence management in the fight against terrorism (13980/04); and Prevention of, and fight against, Terrorist Financing through measures to improve the exchange of information, to strengthen transparency and enhance the traceability of financial transactions (13982/04).

Chapter 3, and in relation to data protection, Chapter 4. In Chapter 5 we examine the complex structures at EU level for combating terrorism, which have developed rapidly in recent years and, as it appears to us, without sufficient co-ordination. It would be absurd to think that action nationally or within the EU alone is a sufficient response to international terrorism and so in Chapter 6 we look at the global dimension. In Chapter 7 we consider the issue of terrorist financing insofar as it impinges on the subject matter of this report.[4] In considering these matters it is important to keep in mind the respective roles of the Member States on the one hand and the Community and Union institutions on the other, in order to help to identify what action can best be taken at the level of the Member States, what requires action at EU level, and where there is a need for EU co-operation at a global level.

4. The inquiry was undertaken Sub-Committee F (Home Affairs) of the Select Committee, whose membership is shown in Appendix 1. We issued a call for evidence in July 2004, which is reproduced in Appendix 2. In conducting our inquiry we took written and oral evidence from a wide range of witnesses, including the Minister of State at the Home Office, Hazel Blears MP, the Secretary General of Interpol, the Information Commissioner, senior police officers, and representatives of non-governmental organisations. We visited Brussels to take evidence from the Commission, the Director of the Situation Centre (SitCen),[5] and the Counter-terrorism Co-ordinator. While we were there we also had discussions with representatives of the Joint Supervisory Bodies responsible for overseeing data protection arrangements in the various Third Pillar bodies which handle personal data.[6] We also visited the headquarters of Interpol in Lyon in order to see at first hand the range of its activities and to get a wider, global, perspective on the fight against terrorism. A list of those from whom we received evidence is at Appendix 3. We are very grateful to all those who assisted our inquiry in this way. We are especially grateful to our Specialist Adviser, Mr John Abbott, the former Director General of the National Criminal Intelligence Service (NCIS), whose wide experience and wise advice were invaluable to us.

---

4 There are many other developments in the EU that are relevant to the fight against terrorism but are outside the scope of this inquiry. In particular, we have not in this report considered relevant EU measures in the area of criminal law, notably the European Arrest Warrant and the Framework Decision on Terrorism, which have been the subject of detailed scrutiny by Sub-Committee E (Law and Institutions).

5 A centre established to undertake common assessments of critical foreign policy issues—see paragraph 51.

6 The Customs Information System, Eurojust, Europol and the Schengen Information System. A note of the discussion with them is at Appendix 5.

CHAPTER 2: BACKGROUND

The terrorist threat

5. Terrorism is not a new phenomenon. But, as Professor Paul Wilkinson[7] explained in his evidence, until recently it was primarily a problem for national governments confronting specific sovereignty/territorial conflicts, such as with the IRA in Northern Ireland and ETA in Spain.[8] Although not without an international dimension, terrorism was not a major preoccupation for the international community. The most significant change in recent years has been the development of global terrorism, of which the leading exponent is the Al Qaeda network: according to Professor Wilkinson it was the emergence of Al Qaeda that changed the situation.[9]

6. The distinctive feature of Al Qaeda and other similar networks is their commitment to variations of a particular brand of fundamentalist ideology based on the teachings of a few masters such as Sayyid Qutb and Abdullah Azzam and dedicated to the eradication of western civilisation.[10] It is this extremist ideology—and the generalised nature of their objectives—that make it impossible to negotiate with them. Moreover, they do not limit their attacks to institutions associated with the State, but seek to attract maximum publicity from high profile attacks, deliberately causing large numbers of civilian deaths. Together with their disregard for their own lives, this makes it much more difficult to put in place effective physical counter-measures.

7. Assistant Commissioner David Veness[11] told us that what is distinctive about developments in recent years is the linkage between different groupings across the world.[12] He said that the most obvious factor linking these groupings were the "Afghan alumni", who had undergone training in camps on the borders of Afghanistan and Pakistan in the period up to October 2002.[13]

8. The event which illustrated most graphically these elements of Al Qaeda's *modus operandi* was the attacks of 11 September 2001 on the World Trade Center in New York and the Pentagon (and the failed attack on an unknown target), when, as Professor Wilkinson pointed out, more people were killed than at Pearl Harbor or in the whole of the Basque terrorist campaign.[14] The bombings in Madrid on 11 March 2004 showed that the Al Qaeda network—or groups inspired by a similar ideology—were equally willing to undertake strikes against European cities and capable of doing so.

---

7 Chairman, Centre for the Study of Terrorism and Political Violence, School of International Relations, University of St Andrews.

8 Q 281.

9 Ibid.

10 See *The 9/11 Commission Report (Final Report of the National Commission on Terrorist Attacks upon the United States*, New York, 2004), page 51.

11 Now Sir David Veness.

12 Q 38.

13 Q 69. Some of this training was initially funded by Western and other agencies during the Soviet occupation of Afghanistan.

14 Q 281.

Proposals on data exchange

Declaration on Combating Terrorism

9. The Madrid attack prompted a special meeting of the European Council on 25 March 2004, which issued the Declaration on Combating Terrorism to which we have already referred.[15] After noting action that had been taken since 9/11, the Declaration identified areas where further work was required. Many of the measures proposed related to the exchange of information—the main focus of this report. The European Council called on the Council of Ministers to examine, among other things, proposals for establishing rules on the retention of communications traffic by service providers and measures for simplifying the exchange of information and intelligence between the law enforcement authorities of the Member States. It urged Member States to ensure that law enforcement agencies exchanged all information relevant to combating terrorism as extensively as possible and invited the Commission to submit proposals for enhanced "interoperability" between European databases. It also called for the flow of intelligence to Europol in relation to all aspects of terrorism to be improved; for the further development of the relationship between Europol and the intelligence services; and for the improved exchange of information on terrorist financing.

Commission proposals

10. In response to the March Declaration the Commission presented a Communication in June 2004 on enhancing access to information by law enforcement agencies.[16] This Communication made proposals for increasing the free movement of information between law enforcement authorities, in particular through the establishment of a principle of "equivalent access to data" between them. This would give law enforcement authorities and police authorities access to data held in another Member State on comparable conditions to those applying to the authorities of that Member State. It also proposed the development of:

- common European standards for authorisation to access classified information;
- "interoperable" and interconnected EU systems; and
- an effective intelligence-led enforcement capability at EU level and the establishment of an EU criminal intelligence network.

Draft Framework Decision

11. Also in June 2004 the Swedish Government tabled a draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, in particular in regard to serious offences including terrorist acts.[17] This instrument, which would put the principle of equivalent access into legally binding form, aims to give police authorities of one Member State access to information and intelligence held by authorities in other Member States

---

15 In paragraph 2 above.

16 Document no. 10745/04.

17 Document nos.10215/04 and ADD 1.

under conditions no stricter than those applicable at national level. It emphasises that it is restricted to "information and intelligence provided to the law enforcement process" and does not extend to information for use as evidence in a criminal proceeding.[18] The draft Decision also contains provisions designed to speed up access to information and establish effective communication channels.

The Hague Programme

12. The "Hague Programme", approved by the European Council on 5 November 2004, sets out the EU's agenda in the field of Justice and Home Affairs for the next five years.[19] It identifies information exchange as one of the key areas for further work and in particular endorses a principle of "availability", whereby information would be available to law enforcement authorities across the EU which needed it on the same basis as to national authorities.[20] We discuss the differences between these approaches in the following chapter.

Commission Communication on police and customs co-operation

13. Improving the flow of information was also one of the main themes of another Communication from the Commission, in May 2004, on enhancing police and customs co-operation.[21] It identified as one of the main underlying problems a reluctance to share information, in particular counter-terrorism information, because of lack of trust between the police and intelligence services. It saw the reluctance of the intelligence services to accept Europol as an equal partner as symptomatic of this. It recommended, among other things, the interoperability of different databases and the designation of Central National Contact Points (CNCPs) for the international exchange of information, which should ideally bring together the Europol national units, the Sirene offices,[22] Customs, the Interpol contact points and representatives from the Judicial Authorities.

Proposals for organisational changes

14. The Declaration on Terrorism also called for greater co-ordination and at its special meeting in March 2004 the European Council decided to make certain organisational changes in the arrangements for co-ordinating the fight against terrorism at EU level, most notably by creating a new post of Counter-terrorism Co-ordinator within the Council. We discuss that post and other institutional issues in Chapter 5.

---

18 Article 1.

19 The Hague Programme is the subject of a separate inquiry by this Committee, conducted jointly by Sub-Committees E (Law and Institutions) and F (Home Affairs).

20 Document no. 14292/04, pages 27-28.

21 Communication from the Commission to the European Parliament and the Council on enhancing police and customs cooperation in the European Union (9903/04).

22 The national bureaux for contact with the Schengen Information System.

CHAPTER 3: INFORMATION EXCHANGE

Information and intelligence

15. Access to information is crucial to countering terrorism effectively. It is equally important that the information is accurate, relevant and timely. We use the term "information" in the widest sense, covering both "hard" data, such as criminal convictions and data on identity documents, and "softer" material, such as evidence of a suspect's associates. Some of this information may be openly available (and the value of such "open source" information should not be overlooked);[23] some may be available in general or specific databases of information, which may be restricted according to their level of sensitivity; some may be information obtained by law enforcement and intelligence agencies from sensitive or secret sources.

16. There is also a distinction between information that can be used as evidence in the courts and information that cannot, either because it is not admissible or because it is precluded by statute from being used. A current example of the latter in the United Kingdom is material derived from telephone interception.[24] "Intelligence" is a term used in a variety of different ways: it may simply refer to the data collected by the security and intelligence agencies, but it is more usually used to connote the interpretation of information. The Commission's Director-General for Justice and Home Affairs defined it as "the first interpretation of information"[25] and it is also sometimes described as "assessed information". Intelligence always needs to be assessed by putting it into context and, where possible, corroborating it.

Exchanging information

17. As international terrorism is a global activity, countering it requires the exchange of information between countries (and not just within the EU). This naturally imports additional difficulties as a result of different national legal and cultural approaches to sharing information. Difficulties inherent in sharing information at national level are likely to be magnified at international level. There may often be good reasons for caution in sharing information: for the intelligence services in particular the protection of sources is paramount; and the originators of intelligence must be confident that the organisation with which it is shared is secure and that it will not be passed on to a third party without their permission. But there may also be less acceptable reasons, such as interdepartmental rivalries and a reluctance to share information for which another agency may take the credit. There may also be inhibitions in some countries about sharing intelligence at the political level.[26]

---

23 Professor Wilkinson made the point that a good deal of material was available in open sources (Q 280); and the Director of the Situation Centre told us that the use of open source information represented a "significant proportion" of its work (Q 177).

24 In a Written Statement on 26 January 2005 the Home Secretary announced that, in the light of a review of the evidential use of intercept material in criminal proceedings, the Government had decided not to remove the existing statutory prohibition on the use of such evidence (*Official Report,* Cols 18-19 WS).

25 Q 121.

26 In his evidence, Mr Whalley (Home Office) said, "…we have a very close linkage between the intelligence community and the civil machinery of ministers. That is not the case in every Member State" (Q 388).

18. We took the opportunity to examine the United States 9/11 Commission Report[27] to see if there were lessons to be learned from it for EU counter-terrorism co-ordination. The Commission was established in November 2002 by the Unites States Congress and the President. The report is a major review of how the terrorist attacks of 11 September 2001 occurred and contains a detailed analysis of the response by the United States Government, its departments and agencies. In its assessment the Report drew attention to, among other things "the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers". It found a "lack of co-ordination within and between agencies", information systems that were "woefully inadequate", and concluded that "everyone involved was confused about the rules governing the sharing and use of information gathered…". It identified human or systemic resistance to sharing information as the biggest impediment to achieving the desired co-ordination through "all-source analysis". Its 41 recommendations include proposals on government and agency co-ordination and information sharing. The shortcomings identified by the Commission occurred in a single, albeit very large, country. It would stretch belief to assume that they are not replicated in the Member States and that, when 25 separate countries are involved, the problems associated with data exchange between them are not considerably magnified.

19. **We have no doubt that more effective sharing of information between law enforcement agencies is crucial to the counter-terrorism effort.**

United Kingdom arrangements

20. We did not receive any evidence of failure by agencies in the United Kingdom to share intelligence with each other or with other Member States. Mr Veness told us that there was a "very effective and close partnership across the boundaries of security service and police work".[28] The Joint Terrorism Analysis Centre (JTAC) based at the Security Service's headquarters brings together representatives of all 11 Government departments and agencies with responsibilities for aspects of counter-terrorism in the United Kingdom and appears to be a model of how different agencies should work together in this field. As we are aware from previous inquiries, the United Kingdom is one of the most active Member States in providing information to Europol, and Mr de Vries confirmed that the United Kingdom was playing a full part in EU counter-terrorism work.[29]

Assessment of proposals

21. The distinction between the different proposals designed to enhance information-sharing and access to information—the Commission's principle of equivalent access, the draft framework decision, and the principle of availability in the Hague Programme—is not clear-cut. The Director-General for Justice and Home Affairs in the Commission told us that the distinguishing feature of the Commission's proposal was the notion of equivalence, i.e. the national rules on access would have to be complied with in each case. He saw this as "slightly more operational" than the Dutch idea

---

27 *Op cit.*

28 Q 63.

29 Q 230.

of availability because it would avoid the need to draw up a set of European safeguards.[30] He understood the Swedish initiative to be designed to improve sharing of information in the short term by imposing an obligation to respond to requests for information from law enforcement authorities and not apply conditions more stringent than would apply to a national request (an idea similar to that of equivalent access).[31] He suggested, however, that it might be more expedient to achieve the same result by amending rules under the Schengen system, without specifying how that might be achieved. Any solution involving the amendment of the Schengen rules would need to take account of the fact that the United Kingdom and Ireland are not full members of Schengen. The draft framework decision is currently still under discussion in the Council.

22. Some of our witnesses were sceptical of these proposals. JUSTICE thought that they were disproportionate.[32] The Chairman of the Eurojust and Schengen Joint Supervisory Authorities (JSAs) described the principle of equivalent access as a "very naïve idea", which would not be practicable unless data were stored in a similar format and without extensive translation facilities.[33] Statewatch thought that the Commission's proposal was unlikely to happen, and that the principle of availability was more likely to be implemented.[34] The police representatives on the other hand thought that they represented the "right direction of travel".[35] The Information Commissioner saw no objection to the principles of equivalent access and availability, provided that exchange of information in accordance with them was necessary and proportionate.[36] The Director of SitCen made it clear that the principle of equivalent access would not apply to "assessed intelligence".[37]

23. Discussion of these issues in the EU often underestimates the considerable amount of information that is already being exchanged on a bilateral and multilateral basis. Simply encouraging the exchange of more information will not necessarily help the counter-terrorism effort: it could even be counterproductive if it led to agencies being submerged in a mass of irrelevant material. It is important to ensure that as far as possible the information exchanged is reliable, relevant and timely. **Nevertheless there is a need to enhance the exchange of information, and the principle of availability offers a suitable framework for doing so. In developing this idea, it will be essential to ensure that the multilateral exchange of information is subject to suitable safeguards; and that it incorporates the idea contained in the principle of equivalent access that information exchanged with other Member States should be subject to the same restrictions as would apply nationally.**

---

30 Q 94.

31 Q 97.

32 Q 2.

33 See Appendix 5.

34 Q 298.

35 Q 58.

36 Q 256.

37 Q 161.

Building trust between agencies

24. Ensuring that agencies exchange information effectively cannot be achieved solely by agreeing general principles such as the principles of equivalent access and availability. Such principles can place a general obligation on agencies—subject to the constraints to which we have referred (such as protection of sources)—to share information with agencies in other Member States on a similar basis to other law enforcement agencies in their own country, but they cannot ensure that that happens without a build-up of knowledge and mutual trust between the agencies. This will not be achieved overnight. **Building mutual trust and confidence within and between agencies, and internationally, is a crucial and continuing challenge to be addressed through positive leadership and effective training.**

25. We recognise that counter-terrorism work is often complex and difficult, and getting more so. The effective use of information at the right time can save lives; failure can cost lives. The increasing "internationalisation" of terrorist networks and activities emphasise the importance of understanding the opportunities and constraints of sharing information, the most effective ways of preventing and investigating terrorism, and the role and capabilities of organisations in different countries and internationally. All our witnesses acknowledged the importance of effective training, which needs to be continuing and aimed at different levels within organisations—operational and strategic—both nationally and internationally. Capacity building and staff exchanges should also be further encouraged. While we acknowledge that some good work in these areas has been undertaken, **we believe that a co-ordinated programme of training, development and work to spread best practice needs to be developed nationally and internationally. CEPOL, the European Police College, based in the United Kingdom at the National Police College, Bramshill, has a valuable role to play here.**

Databases

26. There are already a number of EU databases—the Schengen Information System, the Europol Information System and the Customs Information System—which contain information that may be relevant to counter-terrorism activity, although they also serve a wider purpose. Others are in preparation, notably the second generation Schengen Information System ("SIS II") and a Visa Information System.[38] The Commission has also proposed the development of a centralised European criminal record.[39] More generally both the National Crime Squad and NCIS (the National Criminal Intelligence Service) supported the idea of a central EU database,[40] but the Government were more cautious;[41] and the Commission itself disclaimed any ambitions to establish a centralised system.[42] We share the Government's caution. There is a tendency within the EU to try to solve a problem by creating a new system or database. New databases should only be developed

---

38 Eurojust is also developing a database (p 142).

39 We discussed—and expressed reservations about—this proposal in our report on Eurojust (*Judicial co-operation in the EU: the role of Eurojust*, 23rd Report, 2003-04, HL Paper 138, paragraphs 99-102).

40 pp 150, 151.

41 p 128.

42 Q 105.

if there is a clearly defined need for them and an assurance that they will fulfil their intended purpose. Europol has, for example, experienced a lot of difficulty as a result of some Member States not providing it with the information it needs. Member States need to have a clear incentive to provide information or the database is likely to be seriously incomplete. **We believe that priority should be given to ensuring that existing databases—and those under construction—are effective rather than to developing new ones.**

27. Increasingly information is stored and exchanged in electronic databases. This has enormous advantages for searching and manipulating large quantities of data but means that the databases are vulnerable to the risks that affect all large computer systems, whether computer breakdowns, viruses or external threats. **It is particularly important that databases of information used to combat terrorism are adequately protected and that robust back-up and disaster recovery systems are in place if they should fail.**

"Interoperability"

28. The Commission has also urged that there should be "interoperability" between EU databases. Jonathan Faull, the Commission Director-General for Justice and Home Affairs, defined this as "the ability of two systems to exchange information between themselves and then to process that information further in accordance with their own systems".[43] Where there is a need for information to be exchanged, it clearly makes sense for systems to be able to communicate easily, provided adequate data protection arrangements are in place. However, although we have not examined the technical aspects of interoperability, it seems to us that making existing systems interoperable is likely to be impracticable: ACPO (Scotland) described establishing full interoperability of all law enforcement databases as a "mammoth task".[44] **But, as new systems are developed, the Commission should ensure that there is compatibility between them so that, where it is justified, data can be compared and if necessary exchanged.**

An EU criminal intelligence policy?

29. The Commission's Communication *Towards enhancing access to information by law enforcement agencies*[45] refers to the objective of establishing an EU Information Policy for law enforcement, with the core objectives of providing better information over secure channels for law enforcement co-operation and establishing an effective intelligence-led law enforcement capability at EU level. To achieve the second of these objectives the Commission envisages the development of a European Criminal Intelligence Model. According to the Communication[46] this would encompass "the synchronisation of threat assessment based on a common methodology, systematic underpinning of threat assessment by sectoral vulnerability studies and the required financial and human resource allocation". In its explanatory

---

43 Q 101.

44 p 13.

45 *Op cit*, footnote 16.

46 Paragraph 2.3.

memorandum on the document, dated 6 July 2004, the Home Office stated that the Government were in favour of the Commission's basic proposals for such a model.[47]

30. In its written evidence the Commission seemed to go further, saying that it "saw a clear need to develop a criminal intelligence policy at EU level, especially to prevent terrorism".[48] It saw such a policy as helping to focus and prioritise the efforts of the law enforcement communities of the Member States; enable each Member State to bring its strategic priorities into line with those of other Member States; and allow for the development of shared operational intelligence capacity. In his written evidence the then Home Secretary accepted that there was a need to reach a common view on aspects of the terrorist threat and that EU institutions could therefore benefit from access to assessed intelligence material. But he made it clear that the Government did not see a need for an EU intelligence policy.[49]

31. There is a difficult balance to strike here. There is clearly a need to improve access to necessary and relevant information, encourage the introduction of intelligence-led law enforcement and get all Member States to work more effectively with Europol in respect of serious and organised crime, including terrorism. But this should not extend to action that distorts Member States' own priorities. **We support the development of common standards and sharing of best practice across the EU in this area. But combating terrorism requires a swift, flexible response, which is likely to be hampered by the development of excessively bureaucratic centralised structures. The role of the EU should be one of co-ordination, providing structures to encourage Member States' co-operation, the dissemination of best practice and encouraging the input of information to central databases. There needs to be a clear division of responsibility between the EU and the Member States. In particular, we do not favour an EU criminal intelligence policy, if that implies an EU policy separate from that of the Member States, which would cause confusion and duplication.**

Draft framework decision on the retention of communications data[50]

32. This proposal, which was put forward jointly by France, Ireland, Sweden and the United Kingdom in April 2004, is designed to achieve the approximation of Member States' legislation relating to the retention of communications data as a means of helping to combat crime. Communications data includes telephone and internet subscriber information, itemised call records and mobile phone location data. The proposal does not relate to the content of the data or to the interception of communications. The declared aim of the proposal is to reduce the differences between legislation in the Member States, which are said to be prejudicial to co-operation between law enforcement agencies.

---

47 Paragraph 15.

48 p 34.

49 p 129.

50 Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (document no. 8958/04).

33. Within the United Kingdom the Anti-Terrorism, Crime and Security Act 2001 already provides for the retention of communications data for the purpose of safeguarding national security and any crime directly or indirectly related to it. The Bill originally provided for retention of data for the purpose of fighting crime generally, but was limited to terrorism during the Bill's passage through Parliament.

34. We examined this framework decision in July 2004, when we found it seriously defective in several respects:

- despite its controversial nature, it was not accompanied by a detailed explanatory statement (as it would have been if it had been a Commission proposal);
- its ambit is unjustifiably broad, since under it data would be retained for the purpose of combating crime, without further qualification, rather than serious crime as recommended by the Committee of Privy Counsellors chaired by Lord Newton that reviewed the Anti-terrorism, Crime and Security Act 2001;[51]
- the degree of approximation involved seems half-hearted at best: Member States would be required to retain data for between 12 months and three years, but could derogate from this requirement in relation to certain categories of data and could also have a longer retention period;
- the Information Commissioner did not appear to have been consulted; and
- no Regulatory Impact Assessment was submitted, despite the acknowledged effect on service providers. [52]

35. We expressed these concerns in a letter to the Parliamentary Under-Secretary of State at the Home Office,[53] who has undertaken to provide a regulatory impact assessment. When this is received we shall consider it together with the Government's comments on our other concerns. **We accept that, subject to appropriate safeguards, the retention of communications data may be justified as a weapon in the fight against terrorism and other serious crime but we believe that its application to all crime would be disproportionate.** It may be difficult to draw a satisfactory line between serious and less serious crime, and a regular pattern of smaller crimes may sometimes amount to serious crime, but we would not regard it as acceptable for the police to have unlimited access to this data.

---

51 *Anti-terrorism, Crime and Security Act 2001 review report,* 18 December 2003, HC Papers, 2003-04 100.

52 Our sister committee in the Commons also pointed out that a great deal of communications data relating to UK residents is held by US Service Providers on servers in the United States, where there are no comparable retention requirements.

53 A copy of the letter is at Appendix 6.

CHAPTER 4: DATA PROTECTION

The Data Protection Directive

36. The Community has developed a detailed data protection framework for the First Pillar based on the 1995 Data Protection Directive, which contains detailed rules on, among other things, the principles governing data exchange, supervision, and the transfer of data to third countries.[54] Another significant data protection measure at Community level is a Regulation adopted in 2001 on processing of data by Community institutions.[55] This Directive provided for the establishment of an independent supervisory authority in the Community—the European Data Protection Supervisor. The Supervisor's main task is to ensure that fundamental rights of individuals, in particular their right of privacy, are respected by Community institutions and bodies when processing data. The first European Data Protection Supervisor, Mr Peter Hustinx, was appointed in 2004.[56]

37. However, this comprehensive legislative and regulatory framework does not apply to the Third Pillar. Third (and Second) Pillar activities are explicitly excluded from the scope of the Data Protection Directive. The 2001 Regulation applies specifically to Community (and not Union) bodies, and the tasks of the Data Protection Supervisor are limited to overseeing data protection within the Community framework and by Community bodies.

Data protection in the Third Pillar

38. There is no general framework for data protection in the Third Pillar. Rules on data protection and the supervision of data exchange are contained in the legislation governing the functions of individual Third Pillar bodies such as Europol and Eurojust. Specific data protection rules also govern the operation of the Customs Information System and the Schengen Information System. However, the rules are tailor-made to the functions of each of these systems. Each body and system has its own supervision arrangements, with its own Joint Supervisory Authority (JSA) (Joint Supervisory Body—JSB—in the case of Europol). In the case of Europol, the Customs Information System and the Schengen Information System, members of the JSAs are normally national Information Commissioners from participating Member States. Indeed it is common for the same person to sit on all three JSAs under a different hat (applying different rules). An effort has recently been made to co-ordinate the work of the JSAs by establishing a JSA Secretariat. With Eurojust things are slightly different, as members of its JSA are required to have some judicial capacity/authority in their national administrations.

39. In view of the intensification of data exchange between law enforcement authorities proposed by the Commission and the European Council in order to counter terrorism (and the considerable impact on the rights of the individual that this may have), we examined in detail the issue of data

---

[54] Directive 95/46, OJ L 281, 23.11.1995, p.31. This Directive has been followed by two Directives on data protection in the telecommunications sector and data protection in electronic communications.

[55] Regulation 45/2001, OJ L8, 12.1.2001, p.1.

[56] Mr Hustinx is a deputy judge in the Court of Appeal in Amsterdam, and President of the Dutch Data Protection Authority since 1991.

protection in the area of counter-terrorism co-operation. We focused on three issues in particular:

- the need to develop a specific data protection framework in the Third Pillar;
- the role of national and EU Supervisory Authorities in this context; and
- the framework governing the transfer of data to third countries.

A Third Pillar framework

40. The evidence we received overwhelmingly supported the establishment of an EU framework for data protection in the Third Pillar. According to the Joint Supervisory Authorities, this framework is necessary in view of the processing of personal data on the scale proposed by recent initiatives. The JSAs considered that existing international instruments like the 1981 Council of Europe Convention were too general to provide adequate data protection. In their view a more specific set of data protection rules for police and intelligence authorities should be developed; and simply reaffirming general principles of data protection would not be sufficient.[57] The Commission told us that it would be presenting proposals for data protection legislation for the Third Pillar later in 2005.[58]

41. The JSAs' view was shared by the Information Commissioner, who stressed that the trend towards greater profiling of individuals (rather than exchanging information only on suspects) necessitated a new common legal framework on data protection across the EU.[59] The Information Commissioner advised against the mere transposition of the EC Data Protection Directive to the Third Pillar, noting that the Directive "has its own problems" which should not simply be transplanted to the policing area.[60] Statewatch was similarly critical of the operation of the Directive.[61] The Information Commissioner called for tailor-made standards to apply to the Third Pillar. He noted that the need for a common framework was dictated not only by the need to protect individual rights, but also by the need to facilitate the exchange of information, since the absence of a common EU framework would lead to divergent standards in Member States, which in turn would hinder co-operation.[62]

42. The only evidence we received against the establishment of a common EU data protection framework for the Third Pillar came from the Government. Hazel Blears MP, Minister of State at the Home Office, said that she did not see any strong arguments as yet that a new Europe-wide system would bring added benefit, especially as 23 of the 25 Member States had translated the First Pillar Directive into domestic law.[63] We were puzzled by this argument as the Directive is a First Pillar measure only. The Government's view appears to stem from the belief that data exchange in counter-terrorism is a

---

57 p 148.

58 Q 114.

59 Q 235.

60 Q 260.

61 QQ 297, 300.

62 Q 260, p 73.

63 Q 380.

matter for Member States and not the EU and that it would be undesirable to develop an EU-wide regime that went beyond the national regimes of Member States.[64] However, as the measures contained in the Hague Programme, notably the principle of availability, are implemented, there will undoubtedly be a much greater involvement of the EU in enhancing the exchange of information between national authorities. **In our view enhanced information exchange in the EU, and the trend towards greater profiling of individuals, necessitate the establishment of a common EU framework of data protection for the Third Pillar.** EU standards in this field will contribute towards legal certainty and are necessary to ensure on the one hand that European citizens have confidence that their personal data are processed (and accessed by foreign authorities) lawfully and fairly; and on the other that national authorities have a greater understanding of, and therefore greater trust in, the police practices of other Member States (and are consequently readier to share information with them). **We agree with the Information Commissioner and the Joint Supervisory Authorities that a tailor-made data protection framework for the Third Pillar is necessary. The standards to be adopted should be subject to full parliamentary scrutiny.**

Supervision of Third Pillar data protection arrangements

43. A related issue is supervision of Third Pillar data protection arrangements, especially if and when a common EU data protection framework is developed. As noted above, the current system of supervision in the EU consists of separate arrangements—and a separate supervisory authority—for each EU body. We asked our witnesses whether the existing structures were in need of simplification. The Information Commissioner thought they were, noting that "the proliferation of different legal instruments and supervisory arrangements is confusing, inflexible and disproportionately consuming of the limited resources available to data protection authorities".[65] In his oral evidence, he explained that he was not sure if it was possible to adopt a single set of controls for the various EU databases, since the Schengen Information System was different from Europol, but this did not mean that they could not be supervised by a single supervisory body.[66]

44. The Government also agreed that there might be benefits in bringing together the various supervisory regimes.[67] We also agree. Although there is a need for the specific rules governing specific information systems to be maintained, **there is a strong case for simplifying the existing supervision arrangements at EU level, especially if a specific data protection framework for the Third Pillar is established. If and when the EU Constitutional Treaty enters into force**—which will effectively apply the "Community method" to areas of policy currently in the Third Pillar—**there would be advantage in entrusting supervision for current Third Pillar matters to a central authority.** One possibility would be for the European Data Protection Supervisor to have overall responsibility.[68]

---

64 Q 383.

65 p 73.

66 Q 263.

67 Q 381.

68 It would be impracticable to make such changes in advance of the Treaty because of the complications of the pillared structure and the need in some cases to amend the relevant Conventions.

National supervisory authorities

45. Another important issue is the role of national supervisory authorities in monitoring the exchange of data in Third Pillar matters. Although the 1995 Directive did not cover supervision in Third Pillar matters, many Member States extended their implementing legislation to cover data processing by the police.[69] According to the Information Commissioner this resulted in significant differences in implementation between Member States.[70] In any case, implementation of the Directive did not necessarily result in granting equivalent powers to national supervisory authorities. The Information Commissioner told us that, unlike his counterparts in some Member States, he does not have a power to audit the bodies that he monitors, that is "a power to inspect and audit what is going on"—he has this power only when carrying out his responsibilities as a JSA Member under the Europol and Schengen Conventions.[71]

46. This difference in powers, and the absence of a clear EU legal basis for national supervision in Third Pillar matters, led the JSAs to conclude that, in developing EU standards, steps must be taken to ensure that national authorities have a common legal basis, equivalent powers and sufficient funds and capacity.[72] The Commission was more cautious in saying that the precise powers of national data protection authorities were of concern but the Commission did not want to go too far in examining these powers because some of them were irrelevant in the European context.[73]

47. Notwithstanding this reservation, we believe that, when developing a common EU framework of data protection, the Commission and the Member States should consider the powers and role of national supervisory authorities in supervising the exchange of information between police authorities. Whether it is for the EU or for the Member States to determine precisely these powers, we agree with the JSAs that national authorities should be given enough powers and resources to carry out their duties effectively. In this context, **we believe that it is important that national data protection authorities have sufficient audit powers. We regret that in the United Kingdom the Information Commissioner does not have such powers and recommend that this is reviewed.**

48. Another issue that was flagged up by the supervisory authorities is their input in the development of policy and legislation in the EU on data protection matters. The Information Commissioner pointed out that these authorities did not have any formal role in relation to the proposals forming the subject of this inquiry and that no formal consultation had taken place with national supervisory bodies on the development of the principles in the Hague Programme.[74] This was identified as a shortcoming also by the JSAs, which noted that there is no existing forum in the Third Pillar with the task of advising and assessing initiatives involving the use of personal data. They also noted that the Conference of European Data Protection Authorities recently issued a Resolution calling on the EU institutions to create an appropriate

---

69 p 72.

70 p 73.

71 Q 246.

72 p 148.

73 Q112.

74 QQ 236, 243.

forum for advice and consultation in the Third Pillar.[75] The question of exactly what role the supervisory authorities might have in the development of EU data protection policy needs further examination. **However, we believe that the expertise of these authorities would be very valuable in developing EU policy on data protection and those responsible should make use of it.**

[75] p 148.

CHAPTER 5: EU INSTITUTIONAL STRUCTURES

International co-operation

49. Combating international terrorism, like other serious cross-border crime, requires international co-operation. Informal bilateral and multilateral co-operation between countries with a common interest is well-established: the close co-operation between the United Kingdom and Ireland in relation to Northern Irish terrorism and between France and Spain in combating Basque terrorism are obvious examples. The need for more formal institutionalised co-operation between EU Member States was identified well before the Treaty of Maastricht established police co-operation as a matter of common interest within the newly created European Union in 1991. The Police Working Group on Terrorism (PWGT) was formally established in 1979 in response to terrorist threats from among others the Provisional IRA, the Red Brigades in Italy and the Baader Meinhof gang in Germany. It provides operational communication between police forces at about the level of the Head of the Metropolitan Police Special Branch.[76]

Third Pillar structures

50. Within the Third (Justice and Home Affairs) Pillar there is a separate Terrorism Working Group (TWG), which reports to the Article 36 Committee, a committee of senior officials which has a general coordinating role for Third Pillar matters.[77] At the operational level Europol, the European Police Office, has a particular responsibility for counter-terrorism in its intelligence gathering and analysis role, as does Eurojust, the EU's Judicial Cooperation Unit, in facilitating cooperation between Member States' prosecution services. The Special European Council at Tampere in 1999 decided to set up the Police Chiefs Task Force (PCTF) to co-ordinate high level operational cooperation against serious organised crime, including terrorism. The Task Force currently operates outside normal Council structures but it is planned to associate it more closely with them.

Second Pillar structures

51. The Third Pillar structures have counterparts in the Second (Common Foreign and Security Policy) Pillar with an orientation towards foreign ministries and Member States' external intelligence services. The Second Pillar activity stems from the Amsterdam Treaty, which came into force in October 1999 and established the post of Secretary General High Representative, which has been held since then by Mr Javier Solana. A Situation Centre (SitCen) was established to undertake common assessment of particularly critical issues in terms of the Union's foreign policy. The Centre's assessments are not confined to terrorism. According to Mr William Shapcott, the Director of the Centre, the events of 11 March 2004 had the effect of precipitating closer co-operation between external services and the Centre.[78] Co-operation between internal intelligence services is facilitated by the Counter Terrorism Group (CTG), a group bringing together Member

---

76 Q 39.

77 The Committee's remit is set out in Article 36 of the Treaty on European Union, hence its title.

78 Q 152.

States' Security Services outside Council structures.[79] As a result the European Council agreed that from January 2005 a counter-terrorism cell drawn from the CTG should be established within SitCen so that comprehensive assessments could be made drawing on material from both external and internal services.

First Pillar

52. There are also some First Pillar (Community) interests involved in the fight against terrorism, particularly in relation to terrorist financing and money laundering, legislation on which is the responsibility of the Internal Market Commissioner. Generally the Commission, which until 1997 had virtually no role in the area of law enforcement and security, is now fully associated with the work and indeed has generated, in response to requests from the Council and the European Council, most of the proposals which are the subject of this inquiry. The Director-General for Justice and Home Affairs described to us how he was responsible for co-ordinating the interests of all the Commission services with an interest in counter-terrorism matters.[80]

Informal groupings

53. In addition to these formal structures there is also a wide range of more informal bilateral and multilateral groupings of smaller numbers of Member States with a common interest often organised on a geographical basis, such as the Benelux countries, the Salzburg Group (comprising Austria and its neighbours) and the Baltic Sea Task Force.[81] Recently five of the largest Member States (France, Germany, Italy, Spain and the United Kingdom), the so-called "G5" group, have started holding regular meetings on security issues.

Overall co-ordination

54. In March 2004 the European Council agreed that, in order to co-ordinate work in this area more effectively, the Committee of Member States' Permanent Representatives (COREPER), which covers all three Pillars should take on an overall coordination role.

55. In its response to the events of 11 March the European Council established a new post of Counter-terrorism Co-ordinator, to which Mr Gijs de Vries, a Dutch diplomat and former Minister, was appointed. The Declaration on Terrorism of March 2004 describes the responsibilities of this post, in very general terms, as follows:

"The Co-ordinator, who will work within the Council Secretariat, will co-ordinate the work of the Council in combating terrorism and, with due regard to the responsibilities of the Commission, maintain an overview of all the instruments at the Union's disposal with a view to regular reporting to the Council and effective follow-up of Council decisions".

It appears that Mr de Vries does not have a more specific job description.[82]

---

79 The CTG has a similar membership to the Club of Bern (including Norway and Switzerland as well as the 15 pre-enlargement Member States) but the Club of Bern has a wider remit.

80 Q 141.

81 p 129, Q 142.

82 Q 193.

56. In evidence we received several suggestions about the role of the Co-ordinator which tended to emphasise what he should not do. Mr Veness argued that he should not assume an external or quasi-ambassadorial role, but concentrate on his internal co-ordinating role.[83] The Commission stressed that he should not co-ordinate operational action or seek to co-ordinate Europol's activities, but should monitor the level of compliance by Member States with measures agreed by the Council.[84] Eurojust also emphasised that it was not an operational role, but saw it as building a bridge between the national operational authorities and the EU bodies (and also having an ambassadorial role).[85] We agree that internal co-ordination should be the main focus of the Co-ordinator's work. We also consider that he should have a more detailed job description that provides less scope for ambiguity than at present. Mr Veness, somewhat understatedly, described the description in the Declaration as "a mite generic" and added that "there will be great benefit in tying down those terms of reference with a greater degree of precision".[86]

57. Monitoring implementation of agreed measures is also important. The Member States have a poor record in implementing Third Pillar measures on time, including some which are important for the fight against terrorism. The Hague Programme refers to three Protocols to the Europol Convention, the earliest dating back to 2000, the Convention on Mutual Assistance in Criminal Matters of 29 July 200, and the Framework Decision of 13 June 2002 on Joint Investigation Teams, none of which had been implemented at the time the Programme was adopted.[87] There is no mechanism for monitoring implementation in the Third Pillar as there is in the First Pillar, where the Commission oversees implementation of legislative measures and can take a Member State to the European Court of Justice if it fails to implement legislation.

58. There has been some criticism of what is seen as the lack of the Co-ordinator's accountability. Mr de Vries explained that his accountability was to the Secretary General of the Council, Mr Solana, and through him to the Council, but that he regularly visited the European Parliament and had discussions with the relevant committees there.[88]

59. **The Co-ordinator has a vital role in overseeing the work of the various EU groups and committees within the Second and Third Pillars in order to prevent overlap, avoid duplication and ensure that their aims and objectives are delivered; and in monitoring the implementation of agreed measures. He should have a clear job description which identifies his primary role as internal co-ordination rather than external representation. His work should be subject to parliamentary scrutiny by national parliaments as well as by the European Parliament: the Government should consult the Committee on how this can best be achieved.**

---

83 Q 77.

84 Q 129.

85 p 144.

86 Q 77.

87 Hague Programme, section 2.3.

88 Q 199.

60. Oversight by the Co-ordinator may not on its own be sufficient to ensure that Member States implement agreed counter-terrorism measures. The Hague Programme identifies the need for the Council to develop "practical measures to facilitate timely implementation in all policy areas".[89] It proposes regular progress reports by the Commission to the Council, evaluation of the implementation of all measures, and a yearly evaluation report by the Commission. We welcome these proposals. **In the counter-terrorism area we believe that there should be critical reviews of Member States' performance in implementing agreed measures and following best practice in relation to sharing information and developing counter-terrorism structures. In the absence of a central authority to undertake such reviews, we recommend that they should take the form of a rolling programme of peer reviews by groups of Member States analogous to the peer reviews of Member States' capacity to combat serious organised crime undertaken by the Heads of Europol national units.**

Assessment

61. No-one questions the need for effective co-ordination at EU level of the response to terrorism. But several of our witnesses were critical of the EU structures for achieving this. Mr Veness described it, diplomatically, as "a slightly untidy picture".[90] The Home Secretary said that the Government would like to see "some rationalisation of EU committees dealing with terrorism".[91] **In an area where clarity of roles and responsibilities is vital, we found the structures within the EU for combating terrorism complex and confusing.** Although some of our witnesses promised us a map of all the interlocking and overlapping groups, no one was able to produce one. There is a multiplicity of groups, some within the Second Pillar, some within the Third Pillar, some outside the pillared structure altogether. Some have a policy focus, some an intelligence focus and others an operational focus. The pillared structure of the EU does not help matters and the absorption of most Third Pillar matters into the First Pillar as envisaged by the Constitutional Treaty would be advantageous in this as in other areas, if and when it comes into force. The Constitutional Treaty also makes provision for a Standing Committee within the Council to promote operational cooperation on internal security. Creation of yet another committee will not of itself rationalise and streamline the system which has developed piecemeal, often in response to particular events; but it should provide a better overall co-ordinating body than COREPER, which does not have the time to devote to this important and specialised area. **The Counter-Terrorism Co-ordinator, with his overview of the whole system, has a crucial role to play in ensuring that it works as effectively as possible. We believe that he would be best placed to make recommendations for rationalising and streamlining the present arrangements.**

62. In general we believe that there should be a presumption in favour of working groups in this field operating within Council structures to facilitate co-operation between them and so that they have the support of the Council

---

89 Section II 3.

90 Q 77.

91 p 129.

Secretariat and facilities for meeting in Brussels rather than in Member States. The Commission told us that, if groups like the Police Chiefs Task Force are situated outside the Union's decision-making process, their meetings are not adequately prepared by a staff which is dedicated to their operation.[92] **In this context we welcome the proposal to bring the Police Chiefs Task Force within Council structures.**

Europol

63. Europol should be taking the lead in implementing the EU's response to international terrorism. It is a fully-fledged and well-resourced EU body with a clear legal base; its remit specifically includes crimes committed in the course of terrorist activities; it has a well-established intelligence-gathering and analysis role; and a dedicated counter-terrorism unit has recently been re-established within it. But it is not playing that central role that its position suggests it should. The proliferation of other groups and bodies might not all have been necessary if Europol had established itself as the lead EU player in this area. We were disappointed that in its written evidence Europol itself did not lay claim to a more central role. It was not entirely clear to us why it did not appear to be pulling its weight. In its Communication on police and customs co-operation[93] the Commission suggested that the intelligence agencies did not trust Europol sufficiently to share information with it freely; and we are aware from our own inquiry into Europol two years ago[94] that some Member States' law enforcement agencies do not routinely share information with Europol.

64. We believe that another significant factor is the lack of leadership at the top of the organisation as the result of the long delay in appointing a Director to succeed the previous Director, Mr Jürgen Storbeck, whose appointment expired at the end of June 2004 without any agreement among the Member States as to whether he should be re-appointed or replaced by another candidate. Because of the deadlock three new (and one of the original) candidates) were nominated by Member States, which finally reached agreement on a new Director at the Justice and Home Affairs Council on 24 February 2005.[95] **It is unacceptable that this crucially important post should have been left vacant for eight months as a result of individual Member States insisting on their own national candidates. As the Member States seem to have found it so difficult to reach a consensus on the matter, we recommend that the procedure for appointment should be changed to ensure that the problem does not recur.**[96]

Smaller groupings of Member States

65. Alongside the formal EU structures there are, as mentioned above,[97] groupings of individual Member States including the so-called "G5"

---

92 Q 137.

93 Document no. 9903/04—see paragraph 13.

94 *Europol's role in fighting crime*, 5th Report, 2002-03, HL Paper 43.

95 Mr Max-Peter Ratzel, a senior official in the German Federal Criminal Police Office.

96 We were disappointed to be told by Caroline Flint MP, Parliamentary Under-Secretary of State at the Home Office, when giving evidence in connection with our inquiry into the Hague Programme, that there were no plans to review the appointments procedure (Q 27).

97 In paragraph 53.

grouping. In its evidence the Commission acknowledged that there were many operational matters which groups of Member States wished to discuss in smaller groupings and emphasised that it had no objection to such arrangements. But, Mr Faull added, when it came to policy developments, "only the Union's systems and mechanisms should be used". If it was not possible to reach agreement at 25, the system of enhanced co-operation should be used.[98] The Minister of State at the Home Office, on the other hand, thought that, far from undermining the collective EU effort, such groupings (of which, as she pointed out, the G5 was not the only one) could make progress on specific issues more quickly. She gave the examples of forensics and sharing information which could then be used as examples of best practice.[99]

66. We agree with the Minister. **Despite the proliferation of EU committees Member States retain primary responsibility for counter-terrorism policy and operations, and we believe that they should continue to do so. Protecting a nation's security is arguably the primary responsibility of a government. Co-operating with other Member States, and indeed with governments across the world, is essential in countering terrorism but, if individual countries see a need for a deeper level of co-operation with particular countries with a common interest they should not be debarred from doing so. Nor is there any reason why such co-operation should prejudice work that it is necessary to undertake at EU level with the additional legislative and institutional support that is available there, provided the Member States concerned follow appropriate procedures to keep other Member States fully informed.**

98 Q 142.

99 Q 393.

CHAPTER 6: THE GLOBAL PERSPECTIVE

The international dimension

67. It is natural for EU Member States to focus on the EU and often the impression is given that problems can best be solved by an EU solution. Such an approach is too blinkered, particularly in relation to counter-terrorism. It has become increasingly clear to us as this inquiry has progressed that, insofar as an international response to international terrorism is required, this needs to be organised at global as much as at EU level. The EU must recognise this. The United States is by far the most important player in the international community, and many European countries have close bilateral links with it, not least the United Kingdom, with whom the United States has shared a great deal of its most sensitive intelligence. The EU also seeks to give high priority to co-operation with the US, for example through the EU-US Declaration on Combating Terrorism. There is also an important role for the United Nations in developing anti-terrorism instruments and for the Member States in implementing them.

Interpol

68. There also need to be multilateral fora at the operational level for the exchange of information which may assist in identifying and apprehending terrorists. In this context better use should be made of Interpol, the only global police body. We consider it is a neglected asset, perhaps in part because there is no political element in its structure. In addition to taking evidence from its Secretary General, Mr Ron Noble, we were able to visit Interpol's headquarters in Lyon. We were impressed by the range of Interpol's activities and the potential contribution it could make to the fight against terrorism.

69. Interpol, which has 182 member countries, has the capacity to send immediate response teams in the aftermath of terrorist attacks, and indeed of other civil emergencies (it has taken a leading role in sending teams to some of the countries most affected by the Indian Ocean tsunami in order to co-ordinate victim identification). Its other two core functions are to provide a secure communications system for law enforcement authorities around the world and to manage a series of databases. The communications system known as I-24/7 provides direct access to Interpol's databases 24 hours a day. A 24 hour Command and Co-ordination Centre has recently been set up to monitor events around the world and respond to requests for assistance in the event of urgent investigations or major crises. Interpol's databases include names of wanted and suspected individuals, fingerprints, photographs, DNA, travel documents, and stolen vehicles. Interpol notices provide details of wanted, suspected or missing persons and are colour coded according to the action requested of those who identify them. Red notices, for example, are issued in relation to people whose arrest is requested with a view to extradition. In the counter-terrorism area Interpol has set up in September 2002 the "Fusion Task Force", whose primary role is to identify members of criminal groups engaged in terrorist activity. Since then 13 warning lists containing over 1000 names have been issued; a network of some 187 contact officers has been set up in 117 countries (which do not

include all the EU Member States); and 15 analytical reports have been produced.

70. Given Interpol's large membership comprising a wide range of regimes, data protection is of particular concern. To guard against information falling into the wrong hands Interpol operates a strict rule that a country supplying information may specify with which countries it may be shared and the Secretary General told us that its wishes are strictly respected.[100] The Information Commissioner expressed some concern to us about the robustness of Interpol's data protection arrangements and suggested that it needed to bring them into line with those that apply in the EU and the Asia/Pacific area.[101] There is, however, a Commission for the control of Interpol's files, which checks that the information stored by Interpol is obtained, processed and stored in accordance with Interpol's rules. The Commission also processes requests for access to Interpol's files and carries out spot checks. The Commission is chaired by Mr Hustinx, the European Data Protection Supervisor, and its members include Mrs Elizabeth France, the former United Kingdom Information Commissioner. These arrangements seem satisfactory for protecting the data stored by Interpol, but as Mr David Smith of the Information Commissioner's Office put it, the problem lies with the transfer of data to the member countries. In his view the limited controls in the system inevitably limit Interpol's effectiveness.[102]

Database on lost and stolen passports

71. One of Interpol's databases that could contribute directly to the counter-terrorism effort is that on lost and stolen passports. Terrorists—and international criminals generally—rely heavily on false documentation to assist their movement around the world. Mr Noble told us that in every serious terrorist incident a fraudulent passport has been used.[103] The database contains some 5.6 million items, but we were surprised to learn from Mr Noble that the Schengen Information System (SIS) contains far more, over ten million.[104] **This indicates that many Member States are not notifying relevant information to the Interpol database and probably not consulting it on a regular basis. This is unacceptable. Every effort must be made to ensure that the Interpol database is as comprehensive as possible.** Indeed we question whether there is a need to maintain a separate EU database. The Home Office told us that Europol uses the SIS information for analytical purposes as well as for checks on individual passengers, but as Europol has access to the Interpol database, it would still be able to undertake its analytical work without the need to maintain a separate database. If there were a single global database, it would be in everyone's interest to ensure that it was kept up to date and consulted whenever necessary. At present authorities in the EU may rely instead only

---

100 Q 348.

101 Q 276.

102 *Ibid.*

103 Q 337. Mr Noble gave as an example of the importance of sharing information on lost and stolen passports the passports the case of the man arrested for the assassination of the former Prime Minister of Serbia, Mr Djindjic, on 12 March 2003. He had been travelling on a stolen Croatian passport, on which he had entered six European countries and Singapore and which had been stamped 26 times by immigration authorities.

104 Q 345.

on the passport data in the SIS database, which by definition does not have global coverage.

Council Common Position on the transfer of data on lost and stolen passports to the Interpol database

72. The position may improve significantly as a result of a Council Common Position, which was approved by the Council on 24 January 2005. This measure requires Member States to transmit (non-personal) data on all lost and stolen passports to the Interpol global database. We strongly support this measure, which, if implemented conscientiously, should ensure that the Interpol database is much more comprehensive than at present. This is an interim arrangement until SIS II, the replacement Schengen Information System, is implemented, when it will be possible to exchange the data automatically.

Recording passport numbers on UK landing cards

73. When Mr Noble gave evidence to us he drew attention to the fact that the landing cards completed by foreign nationals on arrival in the United Kingdom, unlike those in most other countries, do not require the passport number to be entered. He suggested that the United Kingdom was losing the opportunity to check the details of those entering the country against the Interpol database.[105] We asked the Minister for her comments on this point. In her reply she explained that, although the Immigration Service does not record the passport number of every third country national, every passport number is "swept" and checked against a hit list of lost and stolen passports.[106] This provides some, but not total, reassurance, since only machine-readable passports can be swept. According to the Minister this gap will be filled in the not too distant future, since, once the "e-borders" programme is fully implemented, landing cards can be dispensed with: sweeping passports will provide all the details required and those without coding will be manually recorded.[107]

Conclusion

74. Interpol performs an important function as the only police organisation with world-wide coverage. In recent years under Mr Noble's leadership its role has developed from what was primarily a post-box function into providing a much wider range of services to the police services of its member countries. Its databases have great potential to assist the identification and apprehension of offenders, and its focus on counter-terrorism in the last two years with the establishment of the Fusion Task Force has the potential to make a significant contribution to the counter-terrorist effort. On the other hand, the very size of the membership imposes limitations on its effectiveness. Intelligence services naturally have concerns about sharing sensitive information despite the ability to restrict the recipients of the intelligence; and the inability to control how other countries handle data

---

[105] Q 337.

[106] p 140.

[107] p 141. In a statement on the Five-year Asylum Strategy on 7 February 2005 the Home Secretary referred to his plans for an integrated system "dealing with people before they enter the UK, at our borders and while they are in the country" (*Official Report,* Col 1183).

places a further restriction. It is unlikely to be possible to overcome completely these obstacles to greater sharing of information, but efforts need to be made to raise global standards of data protection and procedures need to be kept under regular review to ensure that any unnecessary restrictions are removed.

75. Several of our witnesses paid tribute to the work that Interpol does. Mr Veness referred to the way in which it had moved for being an information exchange to "developing particular contributions on a thematic basis", and he described Interpol's work on forged identity documents as "immensely helpful".[108] The Commission told us that there were good relations between EU bodies and Interpol.[109] But Mr Noble clearly felt that the co-operation was mainly one-way: the EU (through Europol and the Schengen Information System) and the Member States have full access to Interpol's databases, but Interpol has no access to the SIS or other EU databases.[110] The Minister acknowledged that Interpol was to some extent the "poor cousin" in comparison with Europol. In her letter of 22 December 2004 she told us that "it is a UK Government priority to exercise influence in the EU so that the institutions develop according to UK interests, making Europol's work of particular significance".[111] There are some promising moves in the direction of closer co-operation, including the proposed link between SIS II and the Interpol database of lost and stolen passports, to which we have already referred, and the posting of a Europol liaison officer to Interpol headquarters.[112] **We strongly believe that there is much to be gained from closer co-operation between the EU, particularly Europol, and Interpol. High priority should be given to enhancing this co-operation and, subject to observing data protection requirements. sharing data more extensively.**

Transfer of data to third countries

76. An issue that is particularly relevant in the context of counter-terrorism at a global level is whether the EU should have common standards governing the transfer of Third Pillar data to third countries. At present there is no general framework in the Third Pillar, only arrangements in relation to specific EU bodies such as Europol. The transfer of data to third countries often gives rise to difficulties. We have given a lot of attention to legislation in this area in the course of our scrutiny work. We have examined a large number of agreements between Europol and third countries on the exchange of personal data and have on occasion been critical of the data protection audit by the JSB. We have also examined the First Pillar agreement between the Community and the United States on the exchange of Passenger Name Record (PNR) data—data held in airlines booking systems to which the US authorities were seeking to have access in order to check the details of passengers before they travelled to the United States. That agreement depended on a prior decision on the adequacy of the US data protection system. We expressed our concern that this "adequacy" decision was taken

---

[108] Q 52.

[109] Q 104.

[110] Q 347.

[111] p 140.

[112] Q347.

by a comitology committee[113] and never deposited for scrutiny with Parliament.

77. The Commission told us that the development of common EU rules in this area was a priority for them and that they would be making proposals in the course of the year.[114] The Government recognise that it would be for the Commission to establish that common standards for the transfer of data to third countries were appropriate but consider that it would be difficult and time-consuming to reach consensus on this.[115] **Notwithstanding these difficulties, and in view of the intensification of information exchange between national authorities in the EU (according to the principle of availability), we believe that it is essential that the EU has a common approach, with high standards, for transfer of data to third countries.** As the Information Commissioner noted:

"It would be unacceptable if UK restrictions on the transfer of data from the UK police to the police in country X could be avoided by the police in another EU Member State, where there are no such restrictions, accessing the UK data and then making the transfer to country X themselves."[116]

78. **Any decision on the arrangements to transfer data to third countries should be subject to full parliamentary scrutiny.** It would be regrettable if the First Pillar precedent, where decisions on the adequacy of the data protection system in a third country are taken not via the standard EU legislative process, but by a "comitology committee,[117] were transferred into the Third Pillar.

---

113 A committee of national experts chaired by the Commission. For a discussion of comitology see *Reforming Comitology*, 29th Report, 2002-03, HL Paper135.

114 Q 114.

115 Q 383.

116 p 73.

117 See footnote 113.

CHAPTER 7: TERRORIST FINANCING

Communication on terrorist financing

79. One aspect of counter-terrorist activity following 9/11 has been a focus on tackling the phenomenon of terrorist financing, which includes the financing of both terrorist groups and terrorist activities. Action at EU level has taken the form of two main initiatives: efforts to freeze the assets of organisations and individuals linked with terrorist activities (on the basis of lists agreed by the Council); and expanding the duty of financial institutions to report suspicious transactions related to money laundering to the authorities to include cases where suspect money may emanate from terrorist activities.

80. In October 2004, in response to other items in the Declaration on Terrorism, the Commission published four further Communications relating to the fight against terrorism.[118] Most of these proposals relate to measures such as civil protection and health protection, which are outside the scope of this inquiry, but the Communication on terrorist financing[119] covers different aspects of information exchange—in particular between law enforcement authorities and financial institutions—and we have therefore considered it in the context of this inquiry.

81. The Commission estimates that the Madrid bombings cost the perpetrators a mere €8000, and that transactions to finance terrorist networks generally also have a small monetary value, which makes the detection of financial transactions for the purpose of terrorist financing difficult. However, the Commission argues that further steps must be taken to create a hostile environment for terrorist financing, while taking care to ensure that nationality or religious affiliation does not become a ground for placing a person under suspicion. More specifically, the Commission calls for:

- the improvement of information exchange between various authorities at national level, as well as between police authorities and the private sector;
- efforts towards real time tracking of financial transactions and granting national Financial Intelligence Units (FIUs) full access to dedicated databases in financial institutions;
- enhancing the traceability of financial transactions and prioritising financial investigations in Member States;
- paying attention to transactions outside the normal financial system;
- enhancing the transparency of legal entities and regulating charities that may be abused for terrorist finance purposes; and
- the development of common standards on asset freezing.

82. The EU Counter-terrorism Co-ordinator, Mr de Vries, prepared a background document on terrorist finance for the December 2004 European Council. The issues identified in the paper included:

---

[118] See footnote 3.

[119] The fight against terrorist financing through measures to improve the exchange of information, to strengthen transparency and enhance the traceability of financial transactions (13982/04).

- the transition from applying asset freezing measures primarily as a political measure to freezing as a preventive measure, which raises a series of legal questions (ranging from what criteria would be applied for asset freezing and which evidence is needed to freeze to matters of due process and the role of intelligence in the designation process);
- the difference between money laundering and terrorist finance—unlike money laundering, in terrorist finance the acquisition of funds is not an end in itself, and unlike money laundering, terrorist finance usually involves small sums; and
- the need to prioritise EU action in a number of areas, mostly similar to the ones flagged up in the Commission's paper. Mr de Vries's paper emphasises the need to co-operate with international bodies such as the Financial Action Task Force (FATF) and present a co-ordinated EU position both in the FATF and in relations with third countries.

83. The proposals by the Commission and Mr de Vries were to some extent reflected in the conclusions of the European Council on 16-17 December 2004. The European Council invited the Commission to present as soon as possible proposals to prevent misuse of charities and urged Member States to put forward known names of individuals and groups for inclusion in EU lists for asset freezing. It also called for the adoption of best practices in implementing financial sanctions and agreement on the third money laundering Directive (which includes terrorist finance in its scope).

84. The effectiveness of these proposals remains to be seen. On the basis of the papers tabled by the Commission and the Counter-terrorism Co-ordinator, it is evident that tackling terrorist finance, while welcome in the fight against terrorism, is a complex task. The main difficulty in adopting effective measures in the area derives from the fact that terrorist finance may involve very small sums, which renders efforts to trace them via the financial system cumbersome and ineffective.

85. The fact that relevant transactions may involve money which is "clean", i.e. coming from legitimate sources and not from criminal activity, may also complicate matters. Monitoring small scale transactions of money which is not suspected of being the proceeds of crime could lead to extensive controls on all customers of financial institutions. This could well be disproportionate and place an unacceptable burden on the financial system. On the other hand if a risk-based approach targeting specific individuals is adopted, the risk of racial and religious discrimination may be increased.

86. The Commission Communication floats the possibility of extending existing controls, by calling on Member States to examine the possibility of granting financial intelligence units (FIUs) direct access to financial databases. Such a move would raise major issues of privacy and proportionality. At present financial institutions are obliged to report suspicions to FIUs, but the current proposal seems to envisage a reversal of the status quo by establishing a "pull" system allowing FIUs to have direct access (maybe in real time) to financial transactions.

87. Another difficulty in addressing the financial dimension of terrorism is the fact that many of the transactions involving terrorist finance may take place outside the conventional financial system. The Commission Communication

refers in detail to informal money remittance systems, such as Hawala,[120] and calls for strengthening the regulatory regime for such systems through the registration and licensing of those transmitting money in accordance with them. It also makes proposals on asset freezing and the position of charities.

88. We do not make any recommendations on asset freezing and restrictions on charities which are outside the scope of this report. But we have considered the proposals relating to access to data. **We support efforts to attack terrorists by targeting their finances, but the difficulties we have described above—the small amounts of money involved, the fact that it may come from legitimate sources, and the difficulty of penetrating informal money transmission networks—are formidable. It would be unrealistic to expect action of this kind to make a major contribution to identifying terrorists and frustrating their operations. Consequently we urge caution, on grounds of both effectiveness and proportionality, in adopting measures that would give financial information units direct access to financial databases**

[120] A traditional remittance system originally developed in India, which operates outside the conventional banking system.

CHAPTER 8: CONCLUSIONS AND RECOMMENDATIONS

Exceptional measures

89. International terrorism represents an exceptional threat to global security. It may require exceptional measures to counter it, although it is vital that such measures are proportionate to the threat and that a proper balance is struck between the requirements of security and the protection of citizens' civil liberties and human rights. Exceptional measures must be clearly directed at the threat. Statewatch has criticised the measures agreed by the European Council following the Madrid attack on the ground that the Council took much of the Justice and Home Affairs agenda on policing and judicial co-operation and relabelled it as anti-terrorism. Statewatch claimed that at least 27 of the 57 proposals had little to do with combating terrorism.[121] It also argued that what was needed was good intelligence on specific threats not mass surveillance of everybody. The problem with that is that it is often the assembly of apparently unconnected pieces of information that provides the good intelligence on a specific threat. However, although we do not accept Statewatch's categorisation of what is and what is not a counter-terrorist measure in its entirety, we agree that measures should be justified as counter-terrorist only if terrorism is their clear target. If such measures are apt to counter other forms of serious crime, they should be justified separately for that purpose. The proposals on the retention of communications data (see paragraphs 32-35) are a case in point.

"Radicalisation"

90. This inquiry has focused on the role of information exchange in better identifying terrorist suspects and preventing terrorist attacks; and the structures within the EU for coordinating action against them. But we have been very conscious of the need also to understand and analyse on a long-term basis the political, religious and social roots of terrorism and the problems of the "radicalisation" of the young.[122] It is important that the ideological foundations of terrorism should be understood so that the pathways which lead from certain beliefs to compulsive acts of violence against those who do not share those beliefs can be identified should be undertaken. **We welcome the intention contained in the Hague Programme to develop a long-term strategy to address the factors which contribute to radicalisation and recruitment for terrorist activities and recommend that this work should include further studies on these intellectual linkages.**

The United Kingdom's contribution

91. We have seen much evidence that the United Kingdom plays a central and positive role in counter-terrorism work across the EU as well as more widely. It makes a major contribution to the work of the EU in this field, not only through the substantial amount of information and intelligence that it

---

121 Q 295.

122 In referring to the problems caused by extremism Mr Veness told us that the support base for terrorism was growing because the causes of tension—in terms of the "geographic, political and other issues which many will dub the root causes"—were growing (Q 67).

provides but through its long experience of counter-terrorism work and the co-ordinated structures it has developed in response to it. It also benefits directly from its involvement with other Member States and the EU institutions. This practical day-to-day cooperation is one of the benefits of being a member of the EU, and the United Kingdom would suffer in these areas if it did not participate wholeheartedly in them.

Summary of recommendations

92. Our specific conclusions and recommendations are reproduced in the following paragraphs.

93. More effective sharing of information between law enforcement agencies is crucial to the counter-terrorism effort (*paragraph 19*).

94. There is a need to enhance the exchange of information, and the principle of availability offers a suitable framework for doing so. In developing this idea, it will be essential to ensure that the exchange of information is subject to suitable safeguards; and that it should incorporate the idea contained in the principle of equivalent access that information exchanged with other Member States should be subject to the same restrictions as would apply nationally (*paragraph 23*).

95. Building mutual trust and confidence within and between agencies, and internationally, is a crucial and continuing challenge to be addressed through positive leadership and effective training (*paragraph 24*).

96. A co-ordinated programme of training, development and work to spread best practice needs to be developed nationally and internationally. CEPOL, the European Police College, has a valuable role to play here (*paragraph 25*).

97. Priority should be given to ensuring that existing databases—and those under construction—are effective rather than to developing new ones (*paragraph 26*).

98. It is particularly important that databases of information used to combat terrorism are adequately protected and that robust back-up and disaster recovery systems are in place if they should fail (*paragraph 27*).

99. As new systems are developed, the Commission should ensure that there is compatibility between them so that, where it is justified, data can be compared and if necessary exchanged (*paragraph 28*).

100. We support the development of common standards and sharing of best practice across the EU in the area of counter-terrorism. However, combating terrorism requires a swift, flexible response, which is likely to be hampered by the development of excessively bureaucratic centralised structures. The role of the EU should be one of coordination, providing structures to encourage Member States' co-operation, the dissemination of best practice and encouraging the input of information to central databases. There needs to be a clear division of responsibility between the EU and the Member States. We do not favour an EU intelligence policy, if that implies an EU policy separate from that of the Member States, which would cause confusion and duplication (*paragraph 31*).

101. Subject to appropriate safeguards, the retention of communications data may be justified as a weapon in the fight against terrorism and other serious

crime, but its application to all crime would be disproportionate (*paragraph 35*).

102. Enhanced information exchange in the EU, and the trend towards greater profiling of individuals, necessitate the establishment of a common EU framework of data protection for the Third Pillar (*paragraph 42)*.

103. We agree with the Information Commissioner and the Joint Supervisory Authorities that a tailor-made data protection framework for the Third Pillar is necessary. The standards to be adopted should be subject to full parliamentary scrutiny (*paragraph 42*).

104. There is a strong case for simplifying the existing supervision arrangements at EU level, especially if a specific EU data protection framework for the Third Pillar is established. If and when the EU Constitutional Treaty comes into force, there would be advantage in entrusting supervision for current Third Pillar matters to a central authority (*paragraph 44*).

105. It is important that national data protection authorities have sufficient audit powers. We regret that in the United Kingdom the Information Commissioner does not have such powers and recommend that this is reviewed (*paragraph 47*).

106. The expertise of the Joint Supervisory Authorities would be very valuable in developing EU policy on data protection and those responsible should make use of it (*paragraph 48*).

107. The Counter-terrorism Co-ordinator has a vital role in overseeing the work of the various EU groups and committees within the Second and Third Pillars in order to prevent overlap, avoid duplication and ensure that their aims and objectives are delivered. He should have a clear job description which identifies his primary role as internal co-ordination rather than external representation. His work should be subject to parliamentary scrutiny by national parliaments as well as by the European Parliament. The Government should consult the Committee on how this can best be achieved (*paragraph 59*).

108. There should be critical reviews of Member States' performance in implementing agreed measures and following best practice in relation to sharing information and developing counter-terrorism structures. In the absence of a central authority to undertake such reviews, they should take the form of a rolling programme of peer reviews by groups of Member States analogous to the peer reviews of Member States' capacity to combat serious organised crime undertaken by Heads of Europol national units (*paragraph 60)*.

109. In an area where clarity of roles and responsibilities is vital, we found the structures within the EU for combating terrorism complex and confusing (*paragraph 61*).

110. The Counter-terrorism Co-ordinator, with his overview of the whole system, has a crucial role to play in ensuring that it works as effectively as possible. We believe that he would be best placed to make recommendations for rationalising and streamlining the present arrangements (*paragraph 61*).

111. We welcome the proposal to bring the Police Chiefs Task Force within Council structures (*paragraph 62*).

112. It is unacceptable that appointment to the crucially important post of Director of Europol should have been left vacant for eight months as a result of individual Member States insisting on their own national candidates. As the Member States seem to have found it so difficult to reach a consensus on the matter, the procedure for appointment should be changed to ensure that the recent deadlock in making the appointment does not recur (*paragraph 64)*.

113. Despite the proliferation of EU committees Member States retain primary responsibility for counter-terrorism policy and operations, and we believe that they should continue to do so. Protecting a nation's security is arguably the primary responsibility of a government. Co-operating with other Member States, and indeed with governments across the world, is essential in countering terrorism but, if individual countries see a need for a deeper level of cooperation with particular countries with a common interest they should not be debarred from doing so. Nor is there any reason why such co-operation should prejudice work that it is necessary to undertake at EU level with the additional legislative and institutional support that is available there, provided that the Member States concerned follow appropriate procedures to keep other Member States fully informed (*paragraph 66*).

114. It is clear that many Member States are not notifying relevant information to the Interpol database of lost and stolen passports and probably not consulting it on a regular basis. This is unacceptable. Every effort must be made to ensure that the Interpol database is as comprehensive as possible (*paragraph 71*).

115. There is much to be gained from closer co-operation between the EU, particularly Europol, and Interpol. High priority should be given to enhancing this co-operation and, subject to observing data protection requirements, sharing data more extensively (*paragraph 75*).

116. It is essential that the EU has a common approach, with high standards, for the transfer of data to third countries (*paragraph 77*).

117. Any decision on arrangements or transfer data to third countries should be subject to full parliamentary scrutiny (*paragraph 78*).

118. We support efforts to attack terrorists by targeting their finances, but the difficulties—the small amounts of money involved, the fact that it may come from legitimate sources, and the difficulty of penetrating informal money transmission networks—are formidable. It would be unrealistic to expect action of this kind to make a major contribution to identifying terrorists and frustrating their operations. Consequently we urge caution, on grounds of both effectiveness and proportionality, in adopting measures that would give financial information units direct access to financial databases (*paragraph 88*).

119. We welcome the intention contained in the Hague Programme to develop a long-term strategy to address the factors which contribute to "radicalisation" and recruitment for terrorist activities and recommend that this work should include further studies on the intellectual linkages with its ideological foundations (*paragraph 90*).

Recommendation to the House

120. In view of the importance of effective co-ordination at EU level in combating terrorism, we recommend this report to the House for debate.

APPENDIX 1: SUB-COMMITTEE F (HOME AFFAIRS)

Sub-Committee F

The members of the Sub-Committee which conducted this inquiry were:

Lord Avebury
†Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Lord Corbett of Castle Vale
Lord Dubs
Baroness Gibson of Market Rasen
*Baroness Harris of Richmond (Chairman)
Earl of Listowel
Viscount Ullswater
Lord Wright of Richmond (Chairman since 23 November 2004)

† From 30 November 2004

* Until 23 November 2004

Mr John Abbott, former Director General, National Criminal Intelligence Service, was appointed as Specialist Adviser for the inquiry.

Declared interests in connection with this inquiry:

Earl of Caithness
Former Minister of State, Foreign and Commonwealth Office

Baroness Harris of Richmond
Former Chair of a police authority and former member of the National Crime Squad Service Authority

Viscount Ullswater
Magistrate on the supplementary list

Lord Wright of Richmond
Former Chairman, Joint Intelligence Committee.

APPENDIX 2: CALL FOR EVIDENCE

Sub-Committee F (Home Affairs) of the House of Lords Select Committee on the European Union is conducting an inquiry into counter-terrorism activities in the EU. It will examine proposals that have been made since the Madrid bombings of 11 March, in particular for changes in the institutional arrangements and for facilitating data exchange within the EU.[123]

Questions on which the Sub-Committee would particularly welcome views include the following:

Justification

- Does the fight against terrorism require much greater operational co-operation and freer exchange of data between law enforcement authorities (both national and EU)?

Data exchange

- The Commission calls for the establishment of the principle of equivalent access to data by national law enforcement authorities in the EU. To what extent would this challenge fundamental legal and constitutional principles of Member States?
- The Commission calls for the interoperability of EU databases. What are the implications of a facility for transferring data between databases? Is there a case for a centralised EU database for all law enforcement purposes?

Data protection

- Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the Third Pillar, as advocated by the Commission?
- Should there be common standards for the transfer of personal data from EU bodies and the Member States to third countries/bodies, including Interpol?

The role of the EU

- Is there a need for an EU intelligence policy, as advocated by the Commission? To what extent can EU objectives be identified separate from those of the Member States?
- How important is it for the EU to speak with one voice in the international arena in matters involving counter-terrorism co-operation?

---

[123] These include a Communication on enhancing access to information by law enforcement agencies (10745/04) and a draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities (10215/04). Also relevant are parts of a Communication on enhancing police and customs co-operation (9903/04); a proposal for a Common Position on the transfer of certain data to Interpol (10475/04); and a draft Framework Decision on the retention of communications data (8958/04).

- The United Kingdom recently hosted a summit of five Member States ("G5") to examine measures to combat terrorism. Do moves of this kind prejudice EU wide initiatives?

Institutional arrangements

- What is the added value of the post of EU Counter-terrorism Co-ordinator? What should his role be?
- What changes are called for in the EU's institutional arrangements (including Eurojust, Europol, the Chief Police Officers' Task Force, and the Terrorism Working Group) in order to combat terrorism more effectively?
- What contribution can EU level training and in particular the EU Police College (CEPOL) make?

28 July 2004

APPENDIX 3: LIST OF WITNESSES

The following witnesses gave evidence. Those marked ⋆ gave oral evidence.

⋆ Association of Chief Police Officers of Scotland (ACPOS), Chief Constable Paddy Tomkins

⋆ Association of Chief Police Officers—Terrorism and Allied Matters (ACPO–TAM), Assistant Commissioner David Veness[124]

⋆ EU Counter-Terrorism Coordinator, Mr Gijs de Vries and Ms Patricia Holland

⋆ European Commission, Directorate-General, Justice and Home Affairs, Mr Jonathan Faull, Director-General, and Mr Joaquim Nunes de Almeida

Eurojust

Europol

⋆ Home Office, Hazel Blears, MP, Minister of State

⋆ Information Commissioner, Mr Richard Thomas, and Assistant Information Commissioner, Mr David Smith

⋆ Interpol, Mr Ron Noble, Secretary General

⋆ Joint Situation Centre, Council of the European Union, Director, Mr William Shapcott

Joint Supervisory Authorities, Europol, Eurojust, Schengen Information System and Customs Information System

⋆ JUSTICE, Dr Eric Metcalfe, Director of Human Rights Police

National Criminal Intelligence Service (NCIS)

National Crime Squad (NCS)

⋆ Statewatch, Mr Tony Bunyan, Chief Editor and Mr Ben Hayes

⋆ Professor Paul Wilkinson, Chairman, Centre for the Study of Terrorism and Political Violence, School of International Relations, University of St Andrews

[124] Now Sir David Veness

APPENDIX 4: GLOSSARY OF ACRONYMS

Glossary of Acronyms

ACPO	Association of Chief Police Officers
ACPOS	Association of Chief Police Officers, Scotland
ACPO-TAM	Association of Chief Police Officers—Terrorism and Allied Matters
CEPOL	European Police College
CIS	Customs Information System
CNCP	Central National Contact Point
COREPER	Committee of Member States' Permanent Representatives
CTG	Counter Terrorism Group
ETA	Euskadi Ta Askatasuna (translates as "Basque Homeland and Liberty")
EIS	Europol Information System
EU	European Union
FATF	Financial Action Task Force
IRA	Irish Republican Army
JSAs	Joint Supervisory Authorities (for Eurojust, and the Customs and Schengen Information Systems)
JSB	Joint Supervisory Body for Europol
JTAC	Joint Terrorism Analysis Centre
NCIS	National Criminal Intelligence Service
NCS	National Crime Squad
PCTF	Police Chiefs Task Force
PNR	Passenger Name Record
PWGT	Police Working Group on Terrorism
SIRENE	SIcherheit in REchnerNEtzen (translates as "Security in Computer Networks")
SIS	Schengen Information System
SitCen	Joint Situation Centre
TWG	Terrorism Working Group

APPENDIX 5: MEETING WITH REPRESENTATIVES OF THE JOINT SUPERVISORY AUTHORITIES RESPONSIBLE FOR DATA PROTECTION IN THE THIRD PILLAR—BRUSSELS, 3 NOVEMBER 2004

Present:

House of Lords

L. Avebury
B. Harris of Richmond (Chairman)
E. Listowel
V. Ullswater
L. Wright of Richmond
John Abbott, Specialist Adviser
Valsamis Mitsilegas, Legal Assistant
Tony Rawsthorne, Clerk

JSA representatives

Mr Emilio Aced Félez, Chairman of the Europol Joint Supervisory Body (JSB) (and Deputy Director of the Spanish Data Protection Control Authority)

Mr Ulco van de Pol, Chairman of the Eurojust and Schengen Joint Supervisory Authorities (JSAs) (and Commissioner on the Dutch Data Protection Commission)

Mr Peter Michael, Secretary to the Europol JSB and Eurojust, Customs and Schengen JSAs

UKREP

Jonathan Sweet
Ben Saoul
Ben Llewellyn-Jones

In the course of their visit to Brussels on Wednesday 3 November members of the Sub-Committee discussed data protection issues relevant to their current inquiry into EU Counter-terrorism activities with representatives of the four JSAs. In his introductory remarks Mr Michael explained the origin and constitution of the JSAs: the chairmanship was held for two years extendable for a further year and did not change with each Presidency; the Council provided facilities for meetings; and in 2001, an independent Data Protection Secretariat was set up, to support the JSAs.

Mr van de Pol said that the JSAs worked closely together, if only because their membership overlapped, but it was worth noting that their first joint meeting had been prompted by the request to submit evidence to the Committee. More generally he observed that data protection restrictions were often blamed for failures of coordination, whereas in fact they were usually due to lack of co-operation between law enforcement agencies stemming from lack of mutual trust. He cited the absence of joint operations as an example of this. The police often dealt in "soft" information and it was important that such information should not be spread too widely: that had been a particular concern with the transfer of Passenger Name Record (PNR) data to the US authorities. Mr Aced Félez said that in general data protection authorities did not simply say no to proposals for

exchanging data: their concern was with rules governing the exchange and the conditions to which the data would be subject.

In response to questions from the Committee Mr Michael said that there was concern about the fact that more data was being exchanged on more subjects and between more law enforcement authorities in the Member States. Often no distinction was drawn between data exchanged for counter-terrorism purposes and for combating organised crime. The JSA representatives were not able to give any examples where information had been misused, but were concerned about the risks inherent in transferring information without clear rules governing its exchange. Mr van der Pol mentioned that they objected to the proposals for the retention of communications data, on the basis that it did not comply with the principle of necessity. It was just a disproportionate proposal.

In relation to interoperability Mr Michael noted that the Schengen JSA had given a formal opinion on the draft Framework Decision on the replacement Schengen Information System (SIS II).

Mr van de Pol described the Commission's proposed principle of equivalent access as a "very naive idea". This would not be practicable unless data was stored in a similar format and without extensive translation facilities. The priority was to make the existing systems work not "dream up" new ones. Mr Aced Félez added that equivalent access was unlikely to be possible at present even within a Member State. He also pointed out that Europol had still not been able to set up the Europol Information System fully. It was, of course, possible to exchange information through Europol but this did not amount to "equivalent access".

The JSA representatives were in favour of a new legal framework for the protection of personal data in the Third Pillar—Mr van de Pol said that there was a need for a common set of principles—but not for a new institution. Mr van der Pol added that there was a need not just for principles but for clear rules. In relation to the SIS, for example, the categories of information were clearly defined but it was still undesirable to put all the information on the system.

Mr Michael said that the most powerful mechanism for exchanging information was the Europol national desks since police officers could talk directly to their opposite numbers. All agreed that training was crucial and that CEPOL could play an important role.

Mr Michael said that there should be a harmonised system for the transfer of data to third countries. Mr Aced Félez added that it was illogical that information could be passed bilaterally to a third country which could not be passed by an EU institution.

As regards the appropriate structure for data protection in the Third Pillar, Mr van de Pol suggested that it needed to be organised on two levels: one within the Council to set the overall rules and the other within each institution. The latter could be achieved either by separate JSAs as at present or by a single body with separate sections for each institution. The Joint Secretariat was very important. He pointed out that it was not difficult to achieve consistency between the JSAs since the composition of all of them was mostly the same. To amalgamate the JSAs would, however, be impracticable: it would take ten years to amend the relevant Conventions. For the moment the JSB representatives saw no major role for the European Data Protection Supervisor, since the exact role of his office was still being developed He was already invited to join the meetings as an observer.

Finally Mr Michael handed over a copy of a Resolution passed at a European Data Protection Conference held in Wroclaw on 14 September 2004 proposing to set up a joint EU forum on data protection and police and judicial co-operation matters.

APPENDIX 6: LETTER DATED 21 JULY 2004 FROM LORD GRENFELL, CHAIRMAN OF THE SELECT COMMITTEE ON THE EUROPEAN UNION TO CAROLINE FLINT, MP, PARLIAMENTARY UNDER-SECRETARY OF STATE, HOME OFFICE

Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism. ("Draft Framework Decision on the retention of communications data") (Document No. 8958/04)

Sub-Committee F (Home Affairs) of the Select Committee on the European Union considered this proposal at a meeting on 21 July.

We found it an unsatisfactory measure in its present form, with no detailed justification for it (other than in your Explanatory Memorandum) and no Regulatory Impact Assessment despite the acknowledged effect it would have on Communications Service Providers.

The proposal is very widely drawn in terms both of the data and services covered and of the purposes for which the data may be retained and accessed. As regards the former, you say that the data will not include the content of communications, but Article 2.2(a) refers to a communication "which includes personal details, contact information and information identifying services subscribed to". It is also unclear what "data necessary to identify the telecommunication in Article 2.2(d) refers to. Article 2.4 is also unacceptably wide in providing that "future technological developments that facilitate the transmission of Communications shall be within the scope of this Framework Decision", which would enable the scope of the Decision to be extended without any further legislative or parliamentary consideration.

The scope of the Decision is stated as covering "crime or criminal offences". You refer to Lord Newton's Committee as supporting such an extension from the provisions of the *Anti-Terrorism, Crime and Security Act 2001*. But that Committee's Report clearly referred to "other *serious* crimes", and we believe that as a minimum the Decision should be limited in this way.

The provision on time periods for the retention of data also seems unsatisfactory for a measure that purports to approximate Member States' laws. The range of the periods permitted, from 12 months to 3 years, is itself very wide, but there are then provisions enabling a Member State either to derogate from the requirement or to extend the periods, subject to only fairly modest limitations.

There is no indication in your Explanatory Memorandum that the Information Commissioner has been consulted, and we would be grateful to know what his views are.

We would also be grateful for a full Regulatory Impact Assessment.

Pending your comments on the points made above and receipt of the additional information requested, the Committee will keep the document under scrutiny. We will also take it into account in our inquiry into EU Counter terrorism activities.

APPENDIX 7: OTHER RECENT REPORTS FROM THE EU SELECT COMMITTEE

Recent Reports from the Select Committee

Session 2003–04

Annual Report 2004 (32nd Report, HL Paper 186)

Session 2004–05

Developments in the European Union: Evidence from the Ambassador of the Grand Duchy of Luxembourg and the European Parliament's Constitutional Affairs Committee (3rd Report, HL Paper 51)

Relevant Reports prepared by Sub-Committee E

Session 2003–04

Strengthening OLAF, the European Anti-Fraud Office (24th Report, HL Paper 139)

Session 2004–05

Procedural Rights in Criminal Proceedings (1st Report, HL Paper 28)

Reports prepared by Sub-Committee F

Session 2002–03

Europol's Role in Fighting Crime (5th Report, HL Paper 43)

The Future of Europe: "Social Europe" (14th Report, HL Paper 79)

Proposals for a European Border Guard (29th Report, HL Paper 133)

Session 2003–04

Fighting illegal immigration: should carriers carry the burden? (5th Report, HL Paper 29)

Handling EU asylum claims: new approaches examined (11th Report, HL Paper 74)

Judicial Cooperation in the EU: the role of Eurojust (23rd Report, HL Paper 138)

Minutes of Evidence

TAKEN BEFORE THE EUROPEAN UNION COMMITTEE (SUB-COMMITTEE F)

WEDNESDAY 20 OCTOBER 2004

Present	Avebury, L	Harris of Richmond, B (Chairman)
	Corbett of Castle Vale, L	Listowel, E
	Dubs, L	Ullswater, V
	Gibson of Market Rasen, B	Wright of Richmond, L

Memorandum by JUSTICE

SUMMARY

1. JUSTICE is a British-based human rights and law reform organisation with 1,600 members. Its mission is to advance justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists.

2. JUSTICE has a history of engagement with EU justice and home affairs issues. In particular, it seeks to ensure that individual rights are adequately protected in tandem with the development of efficient police and judicial co-operation in criminal matters. In addition to this, JUSTICE has undertaken a great deal of work in relation to the human rights implications of counter-terrorism measures.[1] Moreover, the International Commission of Jurists has now identified excessive counter-terrorism measures as a grave threat to the rule of law (see the Berlin Declaration on Upholding Human Rights and the Rule of Law in Combating Terrorism, 28 August 2004).[2]

3. In this submission, JUSTICE highlights the following:

— the importance of counter-terrorism measures that comply with protection for fundamental rights;

— concern over proposals for increased cooperation and data exchange in the absence of common standards and safeguards; and

— the need to ensure existing arrangements are made to work effectively before fresh measures are introduced.

JUSTIFICATION

Does the fight against terrorism require much greater operational cooperation and freer exchange of data between law enforcement authorities (both national and EU)?

4. It seems self-evident that the threat of international terrorism (ie terrorist acts committed on a transnational basis) requires international cooperation among states to combat it. On that basis, efficient operational cooperation and data exchange between law enforcement authorities is something to be promoted. At the same time, though, it is not clear that any failure of national and EU authorities to cooperate and exchange information has been a contributing cause in recent terrorist attacks in the EU (eg Madrid) or against the interests of EU member states elsewhere (eg Istanbul, Bali).

5. JUSTICE notes, for instance, that current arrangements for data transfer exist under the Schengen information system, Europol and the Mutual Assistance Convention. Accordingly, we would caution against the apparent truism that more needs to be done (particularly by way of adopting fresh measures), without first determining whether proper efforts have been made to make existing arrangements work effectively.

6. Moreover, we have concerns that existing EU arrangements for cooperation and data exchange lack the necessary safeguards to protect individual privacy and fundamental rights. The greater the degree of cooperation and exchange of information between EU law enforcement agencies, therefore, the greater the need to protect sensitive personal data from unnecessary intrusion and potential abuse.

[1] See eg JUSTICE response to the Home Office Consultation on Counter-Terrorism Powers, August 2004.

[2] http://icj.org/IMG/pdf/Berlin_Declaration.pdf

7. We also note there is some confusion of aims between measures to combat terrorism and measures to combat serious crime in general. This confusion may be particularly harmful where exceptional measures are justified by way of countering an exceptional threat. While cooperation in the fight against serious crime is also desirable, it is not clear that serious crime poses the same degree of threat to member states.

Data Exchange

The Commission calls for the establishment of the principle of equivalent access to data by national law enforcement authorities in the EU. To what extent would this challenge fundamental legal and constitutional principles of Member States?

8. The central challenge posed by the idea of equivalent access is the lack of equivalent data protection in different EU member states. As we have noted previously,[3] there is little uniformity in data safeguards among member states. Since access to data is determined according to the rules of the requesting state, rather than those of the state providing the information, the ability of each state to protect the privacy of its own inhabitants could be compromised by requests for data from another state with less stringent safeguards.

The Commission calls for the interoperability of EU databases. What are the implications of a facility for transferring data between databases? Is there a case for a centralised EU database for all law enforcement purposes?

9. Again, the ideal of interoperability and the suggestion of an establishment of a centralized database presupposes the existence of common standards and safeguards for data protection and data transfer among EU member states. Different member states gather different information for different purposes, and there is no agreement on what constitutes relevant data in every case. In our view, such common standards would have to be clearly established and firm transnational safeguards put in place before interoperability could be achieved. In particular, there would need to be clear lines of accountability for those involved in operating and using EU databases and an independent authority established to ensure compliance with the relevant safeguards.

10. At the practical level, we consider that greater effort must be made to ensure the *accuracy* of data gathering and storage by national authorities ahead of establishing their interoperability. Without such efforts, the errors of national databases would not be restricted to individual member states but disseminated throughout the EU.

11. We do not see the case for a centralised EU database for all law enforcement purposes as being made out. Such a concentration of sensitive personal data on EU citizens and residents would be an obvious interference with the right to individual privacy and could be justified only insofar as it was strictly necessary and proportionate to an identified need. In our view, the need to establish a single database for even the most serious cross-border crime (ie international terrorism) has not yet been clearly established (because it has not been shown that existing arrangements could not be made to work effectively). We therefore doubt that it could ever be possible to show some generalized need sufficient to establish a database for *all* law enforcement purposes.

Data Protection

Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the Third Pillar, as advocated by the Commission?

12. As noted above and in previous submissions,[4] we do not think that current data protection arrangements provide an adequate level of protection for the rights of EU inhabitants. We agree with the Commission's call for a common EU data protection framework. The absence of sufficient safeguards under the Third Pillar compares unfavourably with those provided under the First Pillar, under which the 1995 Data Protection Directive applies, and actions are subject to the scrutiny of the Data Protection Supervisor and the European Court of Justice.

[3] See JUSTICE written evidence on EUROJUST (April 2004), para 11.

[4] *Ibid.*

13. In terms of relevant applicable standards, we note Article 8 of the EU Charter of Fundamental Rights, which recognizes a right to protection of personal data and identifies in particular the principles of (i) the fair processing of data for specified purposes; (ii) with the consent of the person concerned or some other legitimate basis laid down by law; (iii) rights of individual access and rectification, and (iv) compliance subject to control by an independent authority. We also note the provisions of Article 50 of the draft EU constitution, which further provides that European law should establish rules for "the protection of individuals with regard to the processing of personal data by Union Institutions, bodies and agencies, and by the Member States when carrying out activities which come under the scope of Union law". In particular, we would stress the importance of compliance with data protection rules being subject to independent scrutiny (including judicial scrutiny) and control.

Should there be common standards for the transfer of personal data from EU bodies and the Member States to third countries/bodies, including Interpol?

14. Yes. It would be an obvious lacuna in any EU framework to allow EU bodies and individual member states to go unregulated in the transfer of personal data to third countries and other non-EU intergovernmental organizations. The transfer of such data should be brought under the same framework as that established for regulating transfers of data within the EU, including oversight by an independent body, the accreditation of authorized users, and sanctions for misuse.

The Role of the EU

Is there a need for an EU intelligence policy, as advocated by the Commission? To what extent can EU objectives be identified separate from those of the Member States?

15. We do not take a view on this issue at this time. We would, however, caution against the EU seeking to duplicate the work of national intelligence agencies. Although there is undoubtedly a common EU interest in combating international terrorism, this does not necessarily mean that the EU itself is best-placed to coordinate intelligence gathering, for instance. It seems to us that the EU may be better suited to facilitate cooperation between national intelligence bodies in respect of those international terrorist threats that threaten EU member states, whether jointly or severally.

How important is it for the EU to speak with one voice in the international arena in matters involving counter-terrorism cooperation?

16. We do not take a view on this issue.

The United Kingdom recently hosted a summit of five Member States ("G5") to examine measures to combat terrorism. Do moves of this kind prejudice EU wide initiatives?

17. We do not take a view on this issue.

Institutional Arrangements

What is the added value of the post of EU Counter-terrorism Coordinator? What should his role be?

18. The obvious role of the EU coordinator seems clear—to enhance and promote cooperation between member states and coordinate EU counter-terrorism activities. This only begs the question, however, of what EU counter-terrorism activities there are or should be. If the post of EU counter-terrorism coordinator is to be meaningful, we would suggest that the coordinator should help ensure that counter-terrorism measures (both at the national and EU level) do not interfere with respect for fundamental rights, and that any interference with such rights is both necessary in the circumstances and strictly proportionate to an identified threat.

What changes are called for in the EU's institutional arrangements (including Eurojust, Europol, the Chief Police Officers' Task Force, and the Terrorism Working Group) in order to combat terrorism more effectively?

19. We have previously suggested that Eurojust's role be expanded to include monitoring of Europol, including Europol's agreements with non-EU states. We consider this to be analogous to judicial scrutiny of executive actions at the national level, and would improve the efficiency and legitimacy of Europol activities.

20 October 2004

What contribution can EU level training and in particular the EU Police College (CEPOL) make?

20. In our view, a useful contribution of EU level training could be to stress the importance of compliance of counter-terrorism measures with international and regional human rights standards applicable in the EU, including the EU Charter of Fundamental Rights and the European Convention on Human Rights.

Eric Metcalfe
Director of Human Rights Policy
JUSTICE

14 September 2004

Examination of Witness

Witness: Dr Eric Metcalfe, Director of Human Rights Policy, JUSTICE, examined.

Q1 ***Chairman:*** Dr Metcalfe, a very warm welcome to you. Thank you very much indeed for coming to visit us and to represent JUSTICE and for your very interesting paper, which we have all read and will be asking questions on a little later on. I wonder whether I could just remind Members that before they ask questions, they ought to declare any relevant interests they may have in the inquiry that we are doing. Before I start, or ask Dr Metcalfe if he would like to make an opening statement, could I just register that in the past I have been chair of a police authority for a number of years and also I was a member of the National Crime Squad Service Authority. The subject of this inquiry is the examination of a number of proposals designed to strengthen EU counter-terrorism activities and in particular, by increasing data sharing and data exchange between Member States' law enforcement agencies. These proposals raise important issues relating to data protection and also the institutional arrangements within the EU for responding to terrorist threats. That is the background against which we begin our inquiry. So, Dr Metcalfe, I wonder whether you would like to make an opening statement.
Dr Metcalfe: First of all, let me say how pleased we are to have the opportunity to address your Committee on this important issue. In relation to the submission, I feel I should make clear that it was written with the assistance of my colleague, Marisa Leaf, whose is JUSTICE's EU Justice and Home Affairs Officer. I myself am the Director of Human Rights Policy at JUSTICE. My background is primarily with human rights and counter-terrorism. I am, however, familiar with the proposals and the general range of EU activities under the Third Pillar in relation to these proposals and I just wanted to make clear the division of labour within our organisation. I had hoped that we would both be able to appear before this Committee today, but unfortunately Miss Leaf is speaking to one of your sister sub-committees this afternoon and so is preparing for that. I just have a very brief opening statement and that is to draw your attention to the fact that eight weeks ago the International Commission of Jurists, of which JUSTICE is the British section, adopted a declaration on upholding human rights and the rule of law in combating terrorism. In particular, I should like to draw your attention to clause 8 of the Declaration which reads materially as follows: "In the implementation of counter-terrorism measures, states must respect and safeguard fundamental rights and freedoms including, among other things, the right to privacy which is of particular concern in the sphere of intelligence gathering and dissemination. All restrictions on fundamental rights and freedoms must be necessary and proportionate". I feel that this provision is particularly apt for today's discussion because I feel that it draws attention in particular to the concerns that the International Commission of Jurists has had in relation to the extent to which there has been, since 11 September 2001, a proliferation of counter-terrorism measures. There has been concern about the extent to which human rights standards have been perhaps overlooked in that fight, so I feel that this is an important standard to draw attention to.

Q2 ***Chairman:*** Thank you very much indeed and I am sure that we shall keep that to the front of our minds as we go through the inquiry. Thank you for reminding us about that. I wonder whether I could start the questioning then. In your evidence, which was most interesting, you accepted the need to promote efficient operational co-operation and data exchange between enforcement authorities. Do you think that the proposals that we now have before us will achieve that?
Dr Metcalfe: I think that very much depends on the concept of efficiency that you have in mind. I am sorry—that is a lawyer's answer. At first glance, I would agree that proposals such as equivalent access and inter-operability of databases seem like a straightforward means to achieve co-operation. In fact, if you look more closely, I think they are disproportionate measures in this context. What is

unfortunate is that the idea of 'efficiency' has only been understood in terms of ease of use, that is to say that it is easy for a senior police officer to go to the keyboard, press a button and get the information that he or she requires. I think efficiency also has a number of other senses which are also relevant to this discussion. There is the idea of parsimony, that the database should only give the users of the database what information they need, not information which they do not need, nor information which is irrelevant. Another neglected aspect of the idea of efficient transfer of data is the idea that the data should be accurate. There is no point having a massive database which covers all of the EU's 350 million inhabitants, if the data being transferred is not accurate. It would be a mistake to think of efficiency solely in terms of ease of use, the size of the database or the amount of information stored: an efficient system of data exchange is also one which is accurate and provides relevant information. Indeed, if one accepts that one of the goals of a data exchange system is the protection of fundamental rights, then simply to achieve equivalent access without safeguards would also be an inefficient achievement of those goals.

Q3 ***Lord Avebury:*** I was just wondering, listening to you, whether you think that inter-operability of databases is disproportionate full stop, or whether you concede that there might be a case for having a limited degree of inter-operability such that it was technically possible to access any database by the authorities concerned, but that some limitations could be placed on the nature of data that a particular officer would be able to retrieve on the basis of need to know.
Dr Metcalfe: If it were necessary, if it could be shown that inter-operability were necessary to provide the officer with the information that they required, then yes, there would be a case for inter-operability. Our resistance, such as it is, is rather that we do not see that the case has been made out. Inter-operability and equivalent access seem like desirable goals to the extent that they make the exchange of transfer easier; the question is whether they are also necessary goals. Our concerns are more to do with the fact that if you are going to achieve these larger-scale systems, if you are going to achieve easier transfers of data, you also need to put in place safeguards, otherwise it would be disproportionate. I do not think we actually are opposed to inter-operability and equivalent access *per se:* it is more the idea that they should be achieved irrespective of the need to impose necessary safeguards or the idea that they need to be put in place in order for an efficient system of data transfer to be achieved. We would question that line of reasoning.

Q4 ***Chairman:*** Thank you very much. From efficiency we move swiftly to effectiveness and you cautioned against assuming that new measures were needed; first, you ought to find out whether proper efforts have been made to make the existing arrangements work effectively. So how do you think we could improve existing arrangements?
Dr Metcalfe: I should say that there really does need to be a greater emphasis on establishing common standards for the security and accuracy of existing databases, in particular, common safeguards for data exchange. One particular aspect, I suppose, would be much greater co-operation between the joint supervising bodies of the existing data and protection systems that you have under the Third Pillar in relation to Schengen, Europol, and the Customs Information System. In fact, at first glance, you have a wealth of data protection mechanisms in relation to EU institutions and bodies and Europol and so forth. It is only when you look closely and you see that they are applying their own standards in relation to their own fiefdom, such as it is, that you appreciate that there is a problem in that, say, the Customs Information System and Schengen or Europol and Eurojust may not necessarily be applying the same standards because they have different bodies; they might not be working to the same standards.

Q5 ***Chairman:*** Do you have knowledge of that having happened?
Dr Metcalfe: I do not have any particular knowledge and I would go back to what I said at the beginning, that data protection is not my speciality. We are aware of concerns raised by others in the EU, who have pointed to the fact that there is already some cooperation among some of the joint supervising bodies. You have situations where a national supervising authority, such as the Information Commissioner in the UK, is going to be sitting on the joint supervising body for Eurojust and that is a good thing. We should like to see a lot more of that kind of thing, because it is only through that kind of co-operation that you are going to see all the supervising bodies establishing a common standard. At the moment, though, it is still fragmentary and that is what we are primarily concerned about.

Q6 ***Chairman:*** If you have any examples of that fragmentation, it would be enormously helpful to us if you could send them to our Clerk.
Dr Metcalfe: Certainly.

Q7 ***Chairman:*** That would be really helpful. It was a fairly straightforward statement you made and I think that it would be helpful for us to have something to back that up.

Dr Metcalfe: Yes.

Q8 ***Lord Avebury:*** You criticise the arrangements which already exist for setting common standards between supervisory authorities. Have you made any formal proposal for the establishment of a mechanism which would achieve the objective you mentioned, that is to say full exchange and co-operation between supervisory authorities and setting universal standards for each of them to observe.
Dr Metcalfe: What we have done, is supported the Commission's call for the protections that you currently have in relation to the First Pillar, to be put in place for the Third Pillar. Indeed I suspect you may have other questions which address this more specifically, but we would see that as a primary way forward: to put in place the arrangements which are currently in place in the First Pillar for the Third Pillar and that would help the joint supervising bodies to have this common framework. In practice, I think they understand themselves as beginning to establish this common framework, but it is fragmentary.

Q9 ***Lord Dubs:*** May I first of all apologise? I am going to have to leave fairly shortly, so I will not be able to hear all your answers to our questions. May I ask this one? Given the present situation as regards terrorism and perceptions of it, do you think that situation justifies the adoption of exceptional counter terrorism measures?
Dr Metcalfe: Our organisation's official position is that we are agnostic on whether the current measures are justified. The reason we are agnostic on that point is because we simply do not have access to all the relevant information which the government has used to justify the adoption of exceptional measures. I am thinking primarily of the adoption of exceptional measures within the United Kingdom, but if we are reasoning more generally to the idea that there is a generalised terrorist threat after 9/11 to the European Union as a whole and individual Member States—and we have seen examples of that with Madrid—then we are still concerned that there is an absence of publicly available information which would allow us to say whether a particular measure was necessary or whether a particular measure was proportionate, whether it is tailored to the existing threat. We do accept the finding made by the Special Immigration Appeals Commission and also the Court of Appeal in counter-terrorism cases in the United Kingdom that there is, within the European Convention, a public emergency existing in the United Kingdom which is created by the terrorist threat. The necessity for any particular counter-measures, always has to be weighed against particular evidence and, for perhaps good reasons, that information is not publicly available—and as a civil society organisation, we do not have access to it. Quite frankly, we are not able to say with confidence whether exceptional measures are or are not justified. We rely, as far as possible, on independent scrutinising bodies such as parliamentary committees and also, in particular, the Newton Committee, the Privy Counsellors' Committee which reported on the Anti-terrorism, Crime and Security Act 2001. If I might draw your attention to one of the recommendations of the Newton Committee from last December, they said that "[t]he 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 sensitivity of the information sought". Now, the Newton Committee was concerned with data transfer proposals in relation to transferring airline data, primarily to the United States. You will possibly be aware of the concerns expressed in relation to that. We place great weight on reports such as those of the Newton Committee because the Committee had access to the closed information that the government has used to justify exceptional measures. So when a body such as the Privy counsellors makes these kinds of recommendations, we pay a great deal of attention to them. I hope that answers your question.

Q10 ***Lord Wright of Richmond:*** Perhaps at this point, I ought to declare a possible interest in that I was Chairman of the Joint Intelligence Committee 20 years ago; rather an old interest. Have you taken a position on the very difficult and delicate question of information or intelligence from third parties that may have been acquired by torture?
Dr Metcalfe: Yes. The International Commission of Jurists and JUSTICE issued a press release at the beginning of the House of Lords case on 4 October. We are concerned that the United Kingdom has not incorporated the Convention against Torture into domestic law, which would prevent the judicial use of information obtained by torture that has been provided to the United Kingdom by other countries. So we have come out against that and, as you may be aware, the United Kingdom is also reporting to the Committee against Torture in Geneva in mid-November. We have already made submissions to the Committee against Torture to draw their attention to our concerns.

Q11 ***Viscount Ullswater:*** My question is delving a bit more into counter-measures, but before I ask it I think I should declare an interest: I am a magistrate on the supplementary list. You suggest in your paper that there is some confusion of aims between

measures to combat terrorism and measures to combat serious crime in general. May not activities related to terrorism and serious crime be linked in some instances? Do you see terrorism as an exceptional threat where exceptional measures may be needed?
Dr Metcalfe: I think my short answer would be yes to both of your questions. Yes, there are several overlaps between the fight against serious crime and the fight against terrorism. One of the first, most abstract, points is that terrorism itself is a serious crime, so it would make sense to address that as such. Secondly, there is a great deal of evidence to suggest that terrorist organisations are frequently involved in other kinds of criminal activity in order to finance the terrorist activities. For instance, the Newton Committee drew attention to the fact that terrorist suspects have quite often been engaged in credit card fraud in order to finance other activities. However, our submission tried to make clear that the justification of exceptional circumstances in relation to the fight against terrorism—if there is an exceptional threat to the UK—and the exceptional measures which are adopted should be strictly targeted at the fight against terrorism and not the fight against serious crime *per se.* Our concern would be that you should not allow the use of special anti-terrorism powers against people who are committing credit card fraud in general and that is perhaps a difficult distinction operationally: how do you know when you investigate credit card fraud whether the person is actually a terrorist or not? It is the idea that the armoury of powers that you vest in a government to fight terrorism should not then later on be deployed in the fight against crime generally, unless you can show that the particular type of crime that you are fighting presents the same kind of threat. A very well-known instance of this kind of problem arose just last year: there was the arms fair in East London in the Docklands Convention Centre and the stop-and-search powers which were granted to the Police under the Terrorism Act 2000 were employed by the Metropolitan Police to search protesters at the arms fair. Not to question the good faith of the police in that situation, they used the powers that they had available, however it is an instance of special terrorism powers being deployed against protesters where there is in fact no suggestion that they were suspected terrorists. Indeed, the court judgment makes clear, the evidence given by the Metropolitan Commissioner makes clear, that their suspicion was not based on the idea that these particular protesters may have been linked to terrorist organisations, it was the generalised concern that London is a large city and there is always the possibility of a terrorist threat and whenever large crowds gather, they have to take measures. You can see that there is this kind of trickle-down effect from the fight against terrorism to impinging upon what in our view would be a legitimate public protest.

Q12 ***Viscount Ullswater:*** I am interested in your assessment of the threat level. Are you, for instance, saying that threat to life and limb is more serious that threat to undermining society by other ways which serious crime might do with drugs, human trafficking, credit card fraud?
Dr Metcalfe: Those are certainly all serious problems and if I seem too phlegmatic it is that I perhaps have faith in the ability of society to combat such threats without adopting exceptional measures; whereas I can see that the immediate threat to life and limb posed by a potential terrorist attack could, potentially, justify more extreme measures, say shutting down central London if you felt the need to prevent traffic carrying a bomb into central London for instance.
Viscount Ullswater: That is a helpful clarification; thank you.

Q13 ***Baroness Gibson of Market Rasen:*** Society is not combating some of those issues, is it? Trafficking of women and children, for example, is actually increasing throughout the world.
Dr Metcalfe: To address the trafficking point: we were very pleased to see that the latest Asylum and Immigration (Treatment of Claimants) Act 2004 in fact contains new provisions to address the problem of trafficking and we are certainly concerned about that. Indeed, in a separate context, we are doing work in relation to that in relation to our own asylum work and our criminal justice work. I hope that nothing that I say here would be taken to suggest that we should not be fighting trafficking and other serious crime with vigour. The concern I was raising was whether it was appropriate to be using special terrorism powers to address those problems.

Q14 ***Chairman:*** In a sense it is the linkage though from that serious and organised crime which provides the money which supports terrorism, or which can go towards supporting terrorism; and it is that very ill-defined interface of data—where you collect it, how you collect it, what you use it for—that is, I think, at the root of Lady Gibson's concerns. That is something that we must keep in mind and we must define clearly what we mean to say.
Dr Metcalfe: Yes; thank you.

Q15 ***Lord Wright of Richmond:*** The paper which you submitted is quite critical about the development of centralised EU databases and I think one of the other bodies that has given evidence to us, the Association of Chief Police Officers in Scotland, has made the point that it would be a mammoth task. I really want to ask you, not whether it would be effective or

practical, but would it be desirable. Why do you think it is undesirable?
Dr Metcalfe: The undesirability of centralisation, of the agglomeration of personal data, is that the greater the amount of personal information that you store and the greater the numbers involved, to our mind the greater the interference with the right to personal privacy. A centralised database represents a massive agglomeration of personal data and depending on what kinds of information you are storing, everything from eye colour, to health, DNA, particularly DNA information where you are storing so much information relating to an individual, their potential susceptibility to genetic diseases later on in life—

Q16 ***Lord Wright of Richmond:*** Might it not be more effective and easier to control than the bilateral exchange of information between EU states?
Dr Metcalfe: We would say that the very act of storing all that information in one place and then setting up procedures whereby that information can be accessed represents an exponential interference with personal privacy and that in many ways, having lots of little databases around the European Union is in some ways safer, because you have minimised the degree of harm, if there is unauthorised access or abuse of our personal data. If I hack into a database in Scotland, I have infringed the privacy rights of the inhabitants of Scotland; if I hack into the European central database, I have access potentially to everyone in the European Union.

Q17 ***Lord Wright of Richmond:*** That probably leads on rather naturally to the question of data protection and safeguards. You have already answered Lord Avebury's question in which you mentioned your support for the Commission's call for a common EU data protection framework for the Third Pillar, but do you have anything more you want to say about the principles and standards which a framework of that sort might include?
Dr Metcalfe: I could go into detail about the kind of protections that you currently have available under the First Pillar. First of all there is the oversight of the European data protection supervisor monitoring all First Pillar agencies, ironically enough including the First Pillar activities of some of the bodies which carry out Third Pillar activities. So you have the Customs Information System which operates under the First Pillar supervised, as I understand it, by the European Data Supervisor. The 2001 Regulation laid out in a great deal of detail the kinds of rights and protections and safeguards that would attach to individuals and also the obligations which are put on controllers of data. So you have provision for individuals having legally enforceable rights, you have a host of specific obligations put on the controller of data, rules to process data fairly and lawfully and then great detail on what constitutes lawful processing of data: the data has to be adequate, it has to be relevant, you should not store excessive amounts of data, there should be a requirement to take every reasonable step—a very important phrase—to correct, or in certain cases erase, inaccurate or incomplete data. This is all, to a certain extent, old hat in data protection circles generally in the United Kingdom, and indeed within their own spheres Europol and the Schengen system already have regard to these standards in their own joint supervising bodies. There is however a problem in that there has been a lack of standardisation, so when the Schengen supervisory body makes a decision about what constitutes relevant data, that only applies to Schengen, it does not apply to Eurojust.

Q18 ***Lord Wright of Richmond:*** Does not the Council of Europe Data Protection Convention cover all EU states?
Dr Metcalfe: Yes.

Q19 ***Lord Wright of Richmond:*** You comment in your paper on the lack of uniformity.
Dr Metcalfe: Yes.

Q20 ***Lord Wright of Richmond:*** Does the Council of Europe Convention in itself not suggest a uniformity?
Dr Metcalfe: Yes, and in fact it is perhaps an omission from our written evidence that we failed to refer in terms to the 1981 Convention. We would agree that the 1981 Convention provides an important minimum standard for data protection throughout European Union countries, however what is perhaps problematic is that as a Council of Europe Convention, it lacks any framework by which you can ensure coherence. Unlike a domestic law, we have applications by courts and lower courts regulated by appeal to higher courts, and the highest courts are there to provide consistency and coherence across a lot of decision makers. The 1981 Convention established common standards and basically told each and every country to go away and to implement these standards. Apart from a consultative Committee that was established by way of the Convention, there really is not much else there to ensure coherence and consistency across, say, how France applied the Convention and how Spain applied the Convention.

Q21 ***Lord Wright of Richmond:*** Would you agree with the criticism of the Joint Supervisory Authorities that the Convention is too general?

Dr Metcalfe: Yes. Just to build on that point, there are also some significant exemptions, particularly in respect of what this Committee is concerned with. There is an exemption for state security which would obviously cover most counter-terrorism measures for instance.

Q22 ***Lord Avebury:*** You have expressed concern that the existing new arrangements for data exchange lack the necessary safeguards to protect individual privacy and fundamental rights. You quoted earlier on the Berlin declaration of the ICJ and JUSTICE to the effect that states must respect the right to privacy. We would all agree with that, but it does not give you very much guidance on how you would interpret it in the context of our present inquiry. Could you be more specific on how you think the right to privacy fares in relation to the proposed measures and what you would do, if you were in charge, to vary the proposed measures to ensure that this right was safeguarded?
Dr Metcalfe: I think I can probably do no more than say again, that we should like to see the arrangements in respect of the First Pillar put in place for the Third Pillar, that the best starting point for protecting the right to individual privacy in the European Union in relation to the data gathering and the data transfer between law enforcement agencies would be to make sure that the Third Pillar shares equivalent protection with the First Pillar. It would be important to have in place those standards. There has been some suggestion that in fact it might be quite difficult to establish, straight away, common standards across all the joint supervising bodies and it has been suggested as an intermediate step that there should be a lot more co-operation between the joint supervising bodies. We would certainly encourage greater co-operation, but we think that ultimately, as a matter of consistency and coherence, you need to have the same protections across the board. If it appropriate to have the very safeguards that I referred to beforehand in respect of the First Pillar, in respect of those activities, in respect of Eurodac, then I do not see any clear reason, or obvious reason, why they should not also be put in place in relation to Europol and Eurojust and so forth. I appreciate that you were inviting me to give you specifics and I have referred you back to something I said before, but I am happy to go through it further perhaps and talk about the First Pillar protections, if that would assist you?
Lord Avebury: I personally should be interested in any potential infringements that were occurring now. I do not know of any. I think that if there were widespread infringements of people's individual rights or privacy in relation to the current operations of these databases, then we would have heard about it. I am sure that my e-mail inbox would have been full of it, as it is, for example, on the Civil Contingencies Bill at the moment. We are all getting masses of e-mails explaining precisely how the Civil Contingencies Bill violates everybody's civil liberties. If there were actual instances of people's privacy being invaded as a result of the existing inter-operability of the databases, then everybody in this building would know about it. The fact that we do not, indicates that it is unlikely to be occurring.
Chairman: Not necessarily, I would venture. It might be secret and they might know that their privacy was being invaded.

Q23 ***Lord Avebury:*** Then their security is very much better than mine! Maybe this is not the time to go into that sort of detail but it would be useful, if JUSTICE were aware of any such instances if they would let us know about it. May I go on to ask you about your principle that there should be Third Pillar safeguards? You say you recognise that this cannot be accomplished all at once. Do you think it would be possible, in view of your hint that there are intermediate stages that you could transit through, for there to be a road map which would explain how you get from the present operation of the First Pillar safeguards to the Third Pillar? Is that a task for JUSTICE? Or who else, if not JUSTICE, might be able to undertake it?
Dr Metcalfe: Our suggestion would be that it is something that the Commission should be driving and for those reasons, we have welcomed the Commission's suggestions in relation to extending the protections to the Third Pillar. I suppose that it the quickest answer. I am actually quite keen to come back to your earlier comments in relation to the lack of specific evidence for specific complaints. I think the absence of complaints in respect of data protection is not necessarily evidence, or not conclusive proof at least, that there are no violations of individual privacy. One of the greatest problems in relation to most data protection work is that the average individual really does not know what information has been gathered on them in the first place. There are ways that they could find out if they were keen on enquiring, but in general most people have a very low awareness of the kinds of information that is being stored about them, where it is being stored and who it is being stored by—I myself do not know whether I feature on any of these databases,—and as a consequence that very lack of awareness is probably one of the reasons why you do not see a lot of complaints. A violation could very easily take place. It could be unauthorised access of the Customs Information System under the Third Pillar and how would I know if someone had accessed information about when I crossed the border last? So I am not sure the absence of complaints is necessarily indicative of a lack of a problem. We are not suggesting that these databases are in fact being

hacked into; we have no information in relation to that. What we are suggesting, is that it is problematic that different supervisory boards are applying different standards and that in and of itself is problematic, if you are concerned about individual privacy on an EU level. One of the reasons why we refer to the European Union Charter of Fundamental Rights is that, if it is correct that everyone in the EU has the right to protection of their personal data, then that protection should be the same across all European Union countries. Whether that is the case, where you currently have these piecemeal arrangements in place, is open to question. I honestly do not know, but at the same time, I should be surprised if someone were to assert that there were perfectly uniform protection across the European Union at this very time. I should be sceptical of that, given the little that I happen to know about data protection arrangements as they currently stand under the Third Pillar.

Q24 ***Lord Avebury:*** The danger that we might apprehend is not that hackers would go into the databanks and improperly use the information stored about you on one or other of them, but that the authorities possessing the databases would improperly transfer that information to a third party. Is that not it?
Dr Metcalfe: Yes.

Q25 ***Lord Avebury:*** Again, is there any evidence that you know of that this has occurred, that somebody has provided information for one purpose and through being stored on a European Union database, has been unlawfully transferred to another authority and used to the detriment of the individual concerned?
Dr Metcalfe: No, I do not know of any situation where that has happened, although again, that does not necessarily mean that that kind of situation is not occurring. More generally we would highlight perhaps our concerns in relation to the agreement between Europol and the United States, post 11 September, on the transfer of information and that the fact that the transfer of data in that situation was very much an exception to Europol's own otherwise adequate data protection arrangements. So that is the kind of situation: we do not know what kind of information was transferred from Europol, we do not know the details and the specifics and, given that it is related to counter-terrorism activities, it is probably good from one perspective that that information is not publicly available. The secrecy goes with the medium, when you are talking about the fight against counter-terrorism, so the likelihood of a private individual being likely to be able to know about particular infringements is quite low. It would really rely on a whistle-blowers to come forward and to say "I was working in the Europol office and we had request come over from the FBI". I am not aware of that, but we are primarily concerned, as an organisation, with the policy arrangements and the legal arrangements and so long as the legal arrangements are in place and intact and adequate, then it really falls to enforcement agencies for those rules to be followed. The fact that we do not have information about current possible infringements concerns us less than the fact that the arrangements themselves appear to us to be less than adequate.

Q26 ***Lord Corbett of Castle Vale:*** I think you would probably agree that, if we are going to accept this principle of equivalent access to data by the national law enforcement authorities in the EU, we want the next thing to be equivalent data protection in each of the EU countries. One of the things that we are interested in is how you get there, because it implies common standards of course. Do you see the need for greater intervention to achieve this at EU level, say Commission level, to get there?
Dr Metcalfe: Yes.

Q27 ***Lord Corbett of Castle Vale:*** You were talking earlier about perhaps some other pathway there between the existing, separate supervisory boards. If that is the case, and that could be put in place and achieved, would you then be less concerned about the exchange of information on the scale which is envisaged in those proposals?
Dr Metcalfe: I think we will always be concerned about any increase in the scale of information, so long as it has not been shown that it is necessary to increase the scale of information. In relation to the safeguards, yes, we are obviously very much in favour of the European Union taking the lead in ensuring that proper protections are put in place, and yes, I would say that there is a need for greater intervention at the EU level to ensure that EU countries are consistent in their data protection arrangements. Another way of putting this would be to say that, if you had those arrangements in place, if you had those safeguards in place which are currently in place in relation to the First Pillar, then you would already have incorporated, to a large degree, the kinds of human rights protections that we are concerned to see. There is a requirement of course in the First Pillar standards that you do not transfer more information than you need to, that you take all reasonable steps to ensure that the information, the data you are storing, is accurate, that you are under an obligation to allow revisions and retractions and even to erase inaccurate or incomplete data and so forth. So, once you have those First Pillar protections in place, then you have, to a large degree, incorporated the kinds of human rights protections

that we are concerned with, the kinds of protections talked about in Article 8 of the European Charter of Fundamental Rights.

Q28 ***Lord Corbett of Castle Vale:*** You argue in your paper in favour of independent scrutiny and control of data exchange. What form should this scrutiny take? What is new and different about it from what is happening at the moment?
Dr Metcalfe: What is happening at the moment in relation to the Third Pillar activities is that you have these joint supervisory boards which act in relation to Europol and so forth, and they, within their individual areas, do a good job, but there is no over-arching consistency as far as we are aware. Our idea of independent scrutiny would be something along the lines of the European Data Protection Supervisor and, indeed, that role could be extended. The European Data Protection Supervisor's role could be extended into the Third Pillar. Of course it would mean a great many more resources, but, as he currently does in relation to, say, Eurodac, you could see the same over-arching supervisory role being taken in relation to the other joint supervisory bodies. Perhaps it would in effect be less work for him to do, given that most of the preliminary work would have been done by the JSBs, but nonetheless you would have this over-arching figure who was responsible for all data protection within the European Union and that would provide a safeguard. A further safeguard, of course, is judicial scrutiny. We would favour, above the European Data Protection Supervisor, having scrutiny by the European Court of Justice where appropriate on points of law. Obviously you do not want every single fact-based determination to be appealed to the European Court of Justice, but where important points of law in relation to the interpretation of data protection standards arose, then obviously we would regard it as highly appropriate that the European Court of Justice have this ability to scrutinise.

Q29 ***Lord Corbett of Castle Vale:*** Can you just clarify one point for me? You mentioned the European Data Protection Supervisor and it is implicit, is it not, in what you say that you would want that authority to have not just more resources—I take that point—but more powers as well if it is going to do this job?
Dr Metcalfe: Powers of the kind that it currently enjoys in relation to the First Pillar, powers to regulate, to oversee, to inspect what the particular agencies are doing. Now it is possible, I am not certain, that you may need to make certain different arrangements in relation to how you inspect law enforcement agencies' operations, as opposed to the civilian uses of information, but, at the same time, I doubt that those problems are insuperable. I am afraid I do not really have much to offer by way of specific powers that you would give to the European Data Supervisor.

Q30 ***Baroness Gibson of Market Rasen:*** You have a very interesting paragraph in your response to us about the counter-terrorism co-ordinator and I should like to ask whether you could expand a little bit on the role, particularly in relation to the interference of a person's fundamental rights, which you do mention in your response.
Dr Metcalfe: What we had said in our written evidence in relation to the European Union counter-terrorism co-ordinator was really a question of principle. We have not seen, and to be absolutely fair we have not closely been looking at, the operation of the counter-terrorism co-ordinator thus far, but we have not seen a strong case made for there to be a counter-terrorism co-ordinator at an EU level, if only because a lot of the counter-terrorism activities are necessarily shielded from public scrutiny. We do not know, or are not able to know what the Secret Intelligence Service does in this country. So, it was really an open-ended way of saying that were there a need, were the domestic intelligence organisations and the counter-terrorism organisations of each European Union country of the view that there should be European counter-terrorism coordinators, then that would be a good thing, but we ourselves genuinely do not know whether there is a need, or whether any of the national organisations have expressed concerns. So the first was, if you like, again another agnostic "We do not know for certain" answer whether you need a counter-terrorist co-ordinator. More generally, we took the opportunity to discuss the idea of the counter-terrorism co-ordinators, to suggest that following the Berlin Declaration a very important role of someone who is co-ordinating activities among lots of different counter-terrorism agencies would be to make sure that human rights are respected in relation to those activities. There have been suggestions for a similar kind of monitoring body at the UN level through the UN Security Council and indeed the International Commission of Jurists at our conference last year called upon the UN Security Council to establish a convention to ensure that there would be monitoring of counter-terrorism measures in UN countries. This perhaps is an opportunity: if the EU counter-terrorism co-ordinator is developing their role, this could be one thing that they could do, that they could take account of the various different measures that have been taken and also have regard to the need to secure human rights in relation to that. I have to stress again that we have not looked closely at what the counter-terrorism co-ordinator has been doing.

Q31 ***Earl of Listowel:*** Dr Metcalfe, how important is training in the development of a EU- wide counter-terrorism capability?
Dr Metcalfe: I would have to say it would depend on who is being trained and which level of training we are talking about. If we are talking, say, about training of members of domestic law enforcement units, then obviously the training is a very important way of getting across these common standards in each case. If you are talking about training higher up, say, the supervisory and regulatory bodies, in principle training is again a very good idea. However, we do not have any indication that there has been a problem with the lack of training. It is not something that we have been concerned with as an organisation, so in principle, we would agree that training is a very effective way to establish common standards across different countries, but we do not have any practical views on how this should be achieved.

Q32 ***Viscount Ullswater:*** I am really going back to the EU co-ordinator. Would you see that he had a role to play in perhaps initiating best practice methods throughout this now very large European Union with all the new Member States?
Dr Metcalfe: Yes, I would very much agree with that suggestion, particularly in relation to the accession states some of which have only enjoyed liberal democratic institutions for the past 13 years or so. It may be very valuable for those Member States to have the benefit of guidance, best practice and training. This would link back to the question before, that one possible role for the counter-terrorism co-ordinator could be training them on the appropriate standards, at the same time that they are, one presumes, training them in working with the other domestic counter-terrorism organisations in other Member States.
Chairman: If Members have no further questions, could I thank you very much indeed, Dr Metcalfe, for coming and not just talking to your paper but taking our wider questions; it has been most interesting. During the inquiry we shall develop our thoughts on the issues we are considering and your evidence has been a great help in that respect. Thank you once again from all of us.

WEDNESDAY 27 OCTOBER 2004

Present
Avebury, L
Caithness, E
Dubs, L
Gibson of Market Rasen, B
Harris of Richmond, B (Chairman)
Listowel, E
Ullswater, V

Memorandum by Association of Chief Police Officers, Scotland (ACPOS)

Justification

Does the fight against terrorism require much greater operational co-operation and freer exchange of data between law enforcement authorities (both national and EU)?

There is no doubt that the fight against terrorism is an international one and requires an international response. This will necessitate closer co-operation between Member States, although the existing arrangements, if interpreted correctly, seem fit for purpose.

The exchange of information, particularly in relation to matters of national security, does take place, with the Security Service acting as the recipient and central collation point for the majority of such information. Whilst the secure Cluster messaging system linking United Kingdom Law Enforcement Agencies allows information transfer, there is currently no accessible database to allow police forces to interrogate National Security intelligence. The ability to do this would significantly benefit investigations. At European Union level, it may be that the ability to exchange such data should be limited to a body such as Europol, with the ability to monitor investigations in Member States.

Data Exchanges

The Commission calls for the establishment of the principle of equivalent access to data by national law enforcement authorities in the EU. To what extent would this challenge the fundamental legal and constitutional principles of Member States?

Though individual law enforcement agencies throughout the EU will co-operate fully on all aspects of the investigation of terrorist activity, it is unlikely that many would support the concept of equivalent access. This has implications affecting the intelligence gathering process and would impact directly upon the legal and constitutional principles of Member States to some considerable degree.

Currently, Europol undertakes the role of dealing with matters pertaining to criminal intelligence from throughout Europe. This model functions well and has demonstrated an ability to improve the effectiveness and co-operation between Member States.

The Commission calls for the interoperability of EU databases. What are the implications of a facility for transferring data between databases? Is there a case for a centralised EU database for all law enforcement purposes?

The establishment of full interoperability of all law enforcement databases would be a mammoth task. The Schengen Information System provides a model for a degree of integration, though further attempts at closer ties are likely to meet with considerable resistance from most law enforcement agencies and governments of individual Member States.

In the UK, there are occasional difficulties achieving compatibility in the exchange of data between north and south of the border, although the introduction of the Scottish Intelligence Database (SID) has resulted in significant progress being made within Scotland. Similar work in relation to the National Special Branch Information System (NSBIS) is also ongoing and will afford the sharing of terrorist/extremist intelligence across the UK. It is considered likely that there will be legal and practical challenges in the future regarding the population and sharing of intelligence on NSBIS and while the ability to interrogate a similar intelligence system across Europe would be beneficial, it is suggested that the debate would be far better informed from a sound platform and through experience gained from the creation of UK-wide functionality for NSBIS and any SID equivalent.

Whilst crucial to ensure the integrity of each individual system, the existing legislation, with appropriate deliberation and agreement, would require amendment to allow progress of these issues. The associated challenges are considerable although not insurmountable and may be resolved if sufficient political will exists to do so.

Data Protection

Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the Third pillar, as advocated by the Commission?

Provided that the numbers of those staff with responsibility for administering the current data protection arrangements are increased in line with that envisaged by the Commission, there should be no requirement to alter arrangements as they stand at present. While there will be a need to establish a policy to ensure commonality of data protection processes throughout the EU, this may impinge unnecessarily upon individual Member States' legislative arrangements.

Should there be common standards for the transfer of personal data from EU bodies and Member States to third countries/bodies, including Interpol?

Individual Member States will have their own data protection arrangements, and from a UK perspective, to ensure that confidence in the system is maintained, it is crucial that the existing high standards demanded by UK data protection legislation are mirrored in any system overseen or administered by the Commission. The appointment of a Data Protection Officer and Joint Supervisory Body at Eurojust to ensure commonality of standards should be sufficient to monitor the effectiveness and justification for the transfer of data between Member States.

The Role of the European Union

Is there a need for an EU intelligence policy, as advocated by the Commission? To what extent can EU objectives be identified separate from those of the Member States?

Though the threat to Western democracies from international terrorism undoubtedly affects the EU members as a whole, a common EU intelligence policy would be extremely difficult to implement given the varied domestic problems that affect a large number of Member States. To this end, the EU should have a common voice in tackling international terrorism, though it should guarantee individual Member States the freedom to act individually concerning domestic issues.

How important is it for the EU to speak with one voice in the international arena in matters involving counter-terrorism co-operation?

It is extremely important that the EU should be able to present a united front in terms of counter-terrorism co-operation, though this is likely to be restricted to generalisations, as the interests of Member States will occasionally give cause for discussion at a governmental level.

The UK recently hosted a summit of five Member States ("G5") to examine measures to combat terrorism. Do moves of this kind prejudice EU wide initiatives?

Individual Member States should be encouraged to discuss measures designed to counter terrorist operations. The recent "G5" Summit discussed key issues that affect all Member States and these are likely to be the subject of further high level talks. These smaller Summits of influential members can only benefit the EU as a whole, although the accessibility by Member States to the decision making process will determine how they are regarded.

Institutional Arrangements

What is the added value of the post of EU Counter-Terrorism Co-ordinator? What should his/her role be?

The suggestion of a post of Co-ordinator for Counter Terrorism for the EU is one that has considerable merit.

27 October 2004

The main role of the post holder should be to encourage greater co-operation between Member States through the existing arrangements, while identifying areas where individual Member States acting together can best progress investigations to their mutual benefit. Such a post will provide a conduit for the most effective use, on an international scale, of available information so as to maximise the effectiveness of any proposed intervention.

The Co-ordinator's role should include:

- The creation of a definition of terrorism which enables nation states to challenge all of those groups who would threaten our peace by use of violence.
- The ability to bring together lead figures across EU states responsible for CT responses with a view to initiating best practice in their endeavours.
- The responsibility to set standards in terms of training, recruitment, IT systems and standard procedures.
- The responsibility to ensure that appropriate levels of exchange occur between and across States to enable effective operational planning to occur.
- Membership of and responsibility for the secretariat of a strategic high level steering group tasked with implementing a counter terrorist strategy for the EU. Membership of the group should include Europol, Eurojust, CPO Task Force, etc. The steering group should have direct access to the Commission and should be answerable to the Commission for its decisions.
- Access to a level of budget that would enable the necessary charges to be initiated.

What changes are called for in the EU's institutional arrangements (including Eurojust, Europol, the Chief Police Officers' Task Force and the Terrorism Working Group) in order to combat terrorism more effectively?

With due regard to the constitutional and legislative arrangements in place for each Member State, greater co-operation is required across all levels between those responsible for intelligence gathering, the implementation of operational plans and the prosecution of arrested individuals. These processes require to be addressed in a structured manner, so that all the constituent agencies are aware of their responsibilities and how their efforts can best impact upon counter terrorist activities.

Eurojust, whilst a fledgling agency, has the capability to grow and ensure the jurisdiction of member states is addressed in relation to investigations spreading across many borders. Again, Europol is beginning to have an impact in relation to criminal matters, particularly drugs. With expansion and a legislated constitution to accommodate terrorist matters, this organisation could provide the required structure. The Sirene Bureau at NCIS is now linked into other bureaux throughout Europe, under the Schengen Agreement, allowing the ability of Law Enforcement agencies to track persons throughout Europe.

What contribution can EU level training and in particular the EU Police College (CEPOL) make?

It is clear that, whilst Europe continues to expand, our understanding of each other's constitutions and Law Enforcement capabilities requires to be developed. There would be value in training individuals involved in terrorist investigations, to encompass a more complete awareness of how other EU Countries would interact in a cross border investigation. Clearly, this would be limited to senior investigators who would be likely to be involved in such investigations and those responsible for the gathering and transfer of related intelligence.

In the past 18 months, CEPOL has developed its focus, with results demonstrating the positive impact and value it can have for senior police officers from throughout Europe. In addition, the college has fostered a good spirit of co-operation between National Training Centres, encouraging debate on future training needs for senior police officers.

The main difficulty, as recognised by participants and those responsible for training issues in the police environment throughout the EU, is in identifying an audience of appropriately qualified police officers who have a sufficient command of the English language to benefit from the learning opportunities.

William Rae, QPM
Chief Constable
(Hon Secretary ACPOS)

9 September 2004

27 October 2004

Memorandum by Association of Chief Police Officers—Terrorism and Allied Matters (ACPO-TAM)

Summary of Key Points

1. There are other organisations that are engaged in CT co-operation in Europe, besides those that are part of the EU structure. One such, for law enforcement/police is the Police Working Group on Terrorism (PWGT). Some countries, geographically in Europe are not in the EU.

2. The National Terrorism & Extremism Liaison Section (NTELS) based at New Scotland Yard, runs a network of UK Counter Terrorism & Extremism Liaison Officers (CTELOs) in Europe.

3. The exchange of data within the EU would depend on the type of material being passed and its intended use. Sensitive intelligence would only be passed bi-laterally for intelligence purposes.

4. The different legal systems in Europe means that it is easier for some countries to use and pass materially for evidential purposes, for example intercept product, than others.

5. Non-sensitive data could be shared or communally accessed throughout the EU, provided that any applicable data protection requirements were met.

6. There would need to be agreed standards and procedures for data transfer and/or interoperability of databases and compatibility of IT systems. Bi-lateral exchanges may be the best way forward as an initial step with other countries being brought in later.

7. The best method of combating terrorism in Europe is to have strong national CT police and security service structures in place, supported by the EU with complementary matters, such as analytical assistance, training/ best practice, databases etc.

8. The G5 does not prejudice EU-wide initiatives, it suggests them and can act as a driver for them by getting support and agreement from the five countries with the largest CT capability in Europe.

9. The EU institutional arrangements, Europol, European Police Chiefs' Task Force (EPCTF) and the EU CT Co-ordinator should act in support of EU member states by supporting their CT activity but not by seeking to replicate it or by intervening operationally in it.

Justification

1. The fight against terrorism obviously requires close national and international co-operation in order to prevent the no warning mass casualty type attacks, sometimes involving suicide by the perpetrators, which are the cause of such concern at the present time. The most recent example is the bomb attacks on the commuter trains in Madrid on 11 March this year, which killed almost 200 people. It is clear that every effort must be made to prevent terrorist attacks, wherever they may occur and avoid such casualties. A continuous search for improvements in international law enforcement co-operation, including the exchange of data is therefore justified and would, indeed, be expected by the citizens of Europe. However, terrorism in Europe is not, sadly, a new phenomenon and there has been considerable practical co-operation on counter-terrorism issues for many years, certainly before the formation of such organisations as Europol or the European Police Chiefs Task Force (EPCTF).

2. Since 1975 practical operational co-operation and information exchange for UK police on counter-terrorism matters in Europe has been assured by the National Terrorism & Extremism Liaison Section (NTELS) of the Metropolitan Police Special Branch, based at New Scotland Yard. NTELS, as the name suggests is a national unit and belongs to the Police Working Group on Terrorism (PWGT). This organisation, set up in 1979 in the wake of the assassination of the British Ambassador to the Hague, Holland, includes all EU member states as well as Switzerland and Norway and members have a secure communications network for the passage of information. The leaders of all the PWGT counter-terrorist units meet twice a year in the member countries on a rotating basis. It last met in Warsaw, Poland on 27 and 28 May 2004. There was an exchange of operational information, a presentation by the Spanish delegation on the 11 March attacks in Madrid and dates of future meetings were arranged (UK to host in Autumn 2006). In addition, three new EU countries were admitted to permanent observer status, pending full membership of the PWGT.

3. NTELS also runs a network of Counter-Terrorism & Extremism Liaison Officers (CTELOs) in Europe and beyond. These officers are dedicated to co-operation and the exchange of data with our European police colleagues. At present the CTELOs in Europe are based in France, Germany, Benelux, Italy, Austria (covering central Europe & EU accession countries) and Greece. Agreement has been reached and a CTELO will shortly be appointed for Spain and one may be agreed for Turkey.

4. The point to be made is that there is already very close co-operation and exchange of data between law enforcement authorities both within EU structures and outside it. The need to co-operate with countries that are geographically in Europe, but not part of the EU, such as Switzerland and Norway, should also be stressed. The PWGT arose to service a clear need to pass reliable relevant information rapidly on CT issues between European countries, initially in response to the PIRA European campaigns and such international terrorists as Carlos The Jackal or the Baader Meinhof gang in the mid-1970s. This can be done on a bi-lateral or multi-lateral basis. It has since been augmented by other channels such as Europol and the EPCTF. In addition, following CT incidents such as terrorist attacks or police arrest operations, immediate post event ("hot") de-briefs are held with European CT police liaison colleagues by the country affected. This occurred recently following the Madrid attacks on 11 March 2004 and after the arrests in the UK in early August. These de-briefs enable the emerging intelligence picture to be rapidly disseminated and allows European countries to respond appropriately by re-visiting protective security measures, border controls and so on. It also allows new attack techniques or methods of operation, employed by terrorists, to be made known rapidly throughout Europe. It is difficult to see how this could be improved upon within existing national structures and the constraints imposed by the nature of CT intelligence data.

Data Exchange

5. The establishment of equivalent access to data by national law enforcement authorities in the EU and the extent to which it would challenge member states' legal and constitutional principles would depend on the type of data being accessed and the use to which it would be put. There is a great difference between data which is to be used as part of the judicial process (eg in evidence) and that which is to be used for intelligence purposes (eg to determine which subjects might be placed under surveillance or made subject of an investigation).

6. In the UK some material, such as telephone intercept data, cannot be used in evidence and could not be passed to another EU member state for evidential purposes. However, it could be passed for intelligence purposes, as could material emanating from covert human intelligence sources, although in judicial proceedings public interest immunity would usually be sought. Conversely, in other EU member states, where telephone interception is authorised by an investigating magistrate or judge, intercept data can be passed to the UK and can be used by the member state (and the UK) in evidence in judicial proceedings. In addition, UK data, such as records of criminal convictions, material obtained from a police search under a judicially authorised warrant or from a statement made under the Criminal Justice Act provisions can be passed to another EU member state for use in evidence. Consideration must also be given to the "third party rule", whereby organisations can only pass their own (owned) data. Data which belongs to a third party can only be accessed and disseminated with the consent of the third party.

7. There are also different legal conceptions within the EU about the type of data that might be regarded as "evidence" or that which might be regarded as "intelligence" and the weight that it should be accorded. In some judicial systems, the appearance of a person's name and address in the address book of a convicted terrorist might, alone, be sufficient to institute legal measures such as arrest and search. This would not usually be the case in the UK. There are also issues about the reliability of the data concerned, its age, timeliness and assessment.

8. Possible areas for the sharing of, or equivalent access to, databases in the EU law enforcement community could include those databases which do not contain potentially sensitive intelligence. These could include records of criminal convictions, fingerprint records databases or records of identity documents, that have been reported as lost or stolen. These databases could be centralised for use by all EU member states assuming that suitable IT equipment can be obtained and there may be a case for this to assist in rapid and accurate identifications of persons coming to notice. However, it is unlikely that they would be suitable for all law enforcement purposes as they would not contain the more sensitive information. The interoperability of databases would again depend on suitable compatible IT equipment throughout the EU as would the transferring of data between databases. It would also depend on agreed formats and standards for the data being transferred or held. There are differences in European law enforcement standards in some cases. For example in the number of points of comparison for making fingerprint identifications between the UK and Germany. These would also have to be addressed.

Data Protection

9. The routine passing of data from the UK to any future EU owned and administered database(s) would entail some form of guarantee that it complied with the UK's current data protection legislation, in terms of

its veracity, relevance, age, weeding procedures and so on, or some agreed EU alternative. The UK already contributes a great deal to the Europol's CT analytical databases, but the information is still UK owned and it cannot be further disseminated to other EU member states without the consent of the originator in the UK. (In other words the third-party rule still applies and other states do not have free access, only Europol's CT analysts do.)

The Role of the EU

10. It is the generally held view of the police and intelligence services in the UK (and, I believe, most other EU countries) that the best method of combating terrorism is to have strong national CT law enforcement and intelligence organisations in each of the EU member states that can communicate effectively with all of their other European partners. This national security responsibility cannot be abrogated to Europe or other European institutions. Some EU member states will have different intelligence priorities and requirements in the CT sphere (eg Northern Ireland—UK, Corsica—France, Basques—Spain). In addition, the constraints imposed by the different legal systems results in different methods of law enforcement operating practices between member states. Member states also have widely differing CT capabilities. For these reasons it is the view that the EU and related European law enforcement organisations (Europol & EPCTF) should act in support of member states, for example assisting with analysing the intelligence data and maintaining EU crime databases. It is not thought that, in general terms, the EU has separate CT objectives from those of the member states. Nonetheless, an agreed EU intelligence policy on terrorist threats generally acknowledged to affect all member states (ie the threat emanating from Al Qaida related groups) might assist in focussing the collection of data or allocation of resources in those states where the perception of the threat is less acute than others. In this respect it is important that the EU sets a good example within the international arena in terms of CT co-operation, demonstrating best practice.

11. The fourth G5 Counter-Terrorist practitioners (law enforcement) meeting took place in London on 14 and 15 June 2004, together with a joint meeting with the G5 Security Services representatives. This was one of the pre-meetings for the G5 Home Secretary/Interior Ministers meeting in Sheffield on 5 and 6 July. As a result of the CT practitioners meeting, a list of agreed action points was circulated and a copy of this is attached to this document to give some indications of the issues addressed. The aim of the G5 CT practitioners meeting is to examine and develop initiatives to improve CT co-operation and data sharing and to act as a driver for these to be made EU wide in due course, if this is practicable. Once again, the differences in the law enforcement capabilities of the different member states mean that some are able to move faster than others. It is not felt that the G5 prejudices EU wide initiatives, it is intended to develop and assist them. For example in the development of forensic intelligence databases, bi-lateral exchanges are at first being explored with G5 members, who have the forensic capability. It would then be hoped, eventually, to export this EU wide (and possibly beyond) as an example/benchmark of best practice.

Institutional Arrangements

12. In terms of changes in the institutional arrangements of the EU, as far as Europol is concerned, the G5 CT practitioners meetings (law enforcement & security service) made a number of suggestions to improve co-operation with Europol and increase the relevance of its work (This document is attached to this report classified as RESTRICTED.)[5] The most important point is that the EU institutions add value to and assist with the work being carried out by members states and/or find areas that are not covered by them to develop for themselves. They should not seek to replicate work that is already being done or introduce measures that (intentionally or not) increase the workload on member states or potentially hinder their operational ability, by, for example, seeking an independent operational capability or response to incidents in member states. The differences in capability, legislation and operating environments within member states would effectively preclude this. The same is true for the EPCTF or indeed for the EU Counter-Terrorism Co-ordinator. The EU CT Co-ordinator can ensure that all the EU CT activity, spread as it is among different committees dealing with the various aspects of law, immigration, border controls, transportation, and police liaison, is properly co-ordinated and effective. The EPCTF can ensure, in the law enforcement arena, that the resources are made available in their respective countries to staff joint investigation teams (on an EU-wide, multilateral or bilateral basis) to target or deal with identified CT issues or threats affecting two or more member states.

Andrew Welch
Detective Sergeant

14 September 2004

[5] Document not printed here.

27 October 2004

Examination of Witnesses

Witnesses: Assistant Commissioner David Veness, Metropolitan Police, and Chief Constable Paddy Tomkins, ACPOS, examined.

Q33 ***Chairman:*** Good morning gentlemen. It is always a great pleasure to welcome old friends to the Committee. You are very welcome, Mr Veness and Mr Tomkins. Before we start, could you give us your full titles so that we have that on the record?
Mr Tomkins: I am Paddy Tomkins, Chief Constable of Lothian and Borders Police, representing the Association of Chief Police Officers in Scotland.

Q34 ***Chairman:*** What is your role within ACPO?
Mr Tomkins: Today I am representing the Chief Constables' Council. We are constituent members of the ACPO Standing Committee on terrorism and allied matters.

Q35 ***Chairman:*** You are responsible for that within Scotland?
Mr Tomkins: Yes.

Q36 ***Chairman:*** You do not have another title within Scotland?
Mr Tomkins: No, we do not have a separate or parallel structure for terrorism and allied matters. We are members of ACPO in that regard.

Q37 ***Chairman:*** That clarifies a question we had.
Mr Veness: I am David Veness. I have effectively three roles that are probably of relevance. I am the Secretary of the Association of Chief Police Officers, ACPO, Terrorism and Allied Matters Committee, known as ACPO-TAM. Unusually within British policing, that is a body that encompasses England and Wales, Northern Ireland and Scotland, so we speak with one voice on counter-terrorism. I am also the Chairman of the group known as the ACPO Advisory Group, which acts as the operational co-ordination mechanism dealing, as it were, with quick time issues and immediate operational responses, and again that function is across the United Kingdom. The third function of relevance is as Assistant Commissioner Specialist Operations in Scotland Yard, because there are certain functions of that command which historically have been attached to it, particularly protection, security and anti-terrorism, because of the absence of national policing structures for counter-terrorism within the United Kingdom.

Q38 ***Chairman:*** Thank you very much indeed. That has been enormously helpful and members will have much appreciated the fact that we have such experience with us today. Could I then begin by welcoming you and thank you very much for coming and for your evidence, which has been very full and we will be asking questions based on that. We have all read avidly the evidence that you have put before us. I wonder if I could register, for the benefit of members of the public who are now sitting behind you, the subject of the inquiry, which is an examination of a number of proposals designed to strengthen EU counter-terrorism activities, particularly through much more extensive data exchange. These proposals raise important issues relating, among other things, to data protection and the institutional arrangements within the EU for combating terrorism. I hope that has been helpful. Members' interests relevant to the inquiry are being deposited at the back of the room. I wonder whether, before we start questioning, you would like to make any opening statements?
Mr Veness: My Lord Chairman, there are some very brief points which may be helpful in terms of context. The first point is to understand the nature of counter-terrorism, because I think sometimes there is a danger that it is perceived as only focusing on effective intelligence and detection of individuals, whereas I think, particularly in the 37 months since 9/11, it is as important to recognise that dealing with community issues, dealing with the handling of crises, and indeed dealing with the consequences should dire terrorist events unfold are equally important. In many ways those issues have tended to be dealt with separately, both nationally and internationally. Our view is that the cohesive, as it were linear, approach to all of those issues in many ways defines the agendas both as to which nations can contribute and particularly which supra-national bodies can contribute. The strategic challenge would be the first point. The second point is that the way that our world has changed in counter-terrorism in the last 37 months can be summed up in the one word "global", in that hitherto we dealt with an issue which was regional; here within the United Kingdom we understood a threat that emanated primarily from the island of Ireland that was aimed at the GB mainland. That is transparently no longer the case. Every instance that we are engaged in, almost however minor, in this new dimension involves a range of nations, and indeed a range of nations much broader than the European Union. Thirdly, our view is that the gap internationally on the global scale is in relation to national capability and capacity. In our judgment, the key building block is to ensure that each individual country, particularly those which understand that they are afflicted by this new dimension of threat, is responding appropriately and is building effectively from the national level upwards. The fourth issue, very briefly, if we are to

reflect on and be critical of where progress has not been achieved, particularly over the last 37 months, would be the growth of the support networks. This is dubbed the radicalisation debate. I think probably more accurately for radicalisation read extremism because of the nature of the origins of the issue, and indeed the support networks, if anything, sad to relate, are growing rather than diminishing. We would regard that as almost the key strategic challenge in halting that development and ideally reversing it. Those would be the four brief points that I would make.

Mr Tomkins: The only thing I would add, in addition to the points you have already clarified in your kind introduction, is that from Scotland's perspective, we are part of the ACPO structure and therefore we recognise ACPO policy development in this area and the pre-eminence of the Metropolitan Police. There are jurisdictional issues, obviously, as has been referred to, between Scotland and England and Wales, and those, in some ways, govern the operational constraints. That might offer a microcosm of some of the issues that are being explored by this Committee in terms of EU interoperability.

Q39 ***Chairman:*** Thank you very much indeed. I think that leads us very nicely into the first question. As I said, we are most grateful for the papers you were both able to send us. My first question is about the Police Working Group on Terrorism. You have given us quite a lot of information about that. I am very grateful for that because you stress the importance of the role of that group where it deals with counter-terrorism operations in Europe. I just wondered if, for the sake of our report, you would be able to tell us a little bit more about how it operates and whether its members have powers to exchange personal data. How does it link in to other databases? Is there a need for it to do that sort of thing?

Mr Veness: If I may paint the skeleton, this is an unusual body in that it pre-dates most of the other institutions to which we will probably refer. It was born out of tragedies during the 1970s. There were the beginnings of an understanding, particularly when the activities of the Provisional IRA were manifest on the continent of Europe during the 1970s. You will recall that the attacks upon NATO institutions at that time, the Red Brigades, the Baader Meinhof era, were very much novel challenges. There was recognition amongst operational police chiefs of the need to have an effective communication method that dealt with issues at the operational level that was swift, effective and non-bureaucratic. That was the intention. It was formally established in 1979. It now links, in terms of EU membership, the Baltic States plus Malta, the most recent to join.

Q40 ***Chairman:*** Those are the three new ones you refer to?

Mr Veness: Yes, and it will reflect EU membership. It operates, in terms of the actual meeting arrangements, six-monthly in a different nation on each occasion. It last met in Poland in May of this year. There is an imminent meeting, in fact later next week, in Germany of that grouping. Each of the operational services will be represented. It tends to operate at a level which is below that of the European Police Chiefs Task Force. For example, among our UK representatives next week will be the Head of Special Branch within the Metropolitan Police, who is mandated to take forward that role. It is helpful to describe the various operational activities that have flowed from the working group's creation. Within Scotland Yard—but that is only a convenience on behalf of UK policing—the Police Working Group on Terrorism led to a body which is now the National Terrorism and Extremism Liaison Section, and that acts as a post-box by which urgent communication can be initiated, even on the most mundane inquiries—for example, who owns a particular motor car or about a recent crime—within each of the contributing states. Within the United Kingdom, there is that 24-hour capability of linking in with the other constituent organisations. There is then a structure, in terms of deployment of officers, which is known as the Counter-Terrorism and Extremism Liaison System—and I merely refer to the British example—whereby we deploy officers in locations abroad, notably within Europe. There are others in Australia and Canada, but the officers are mainly engaged in the European theatre in order to give us literally the day-by-day liaison that we need with our colleagues engaged in these duties around Europe. The reciprocal dimension of that is that a great many other European nations are generous enough to provide liaison officers to London, so what you see in London, day by day, is team work between the hub, our own National Terrorism and Extremism Liaison Office, and officers mainly from European police forces and other like organisations, who are either on the staff of that body or are in their embassies here in London. They are available in order to give us that direct operational linkage. Of course we would wish that network to be wider and broader and often there is a number of countries covered from one particular location, but that, broadly, is the method of operation.

Q41 ***Chairman:*** Is that hub within Scotland Yard?

Mr Veness: It is, and that, in many ways, is a historical fact because of the original concept. Although it was a combined UK initiative, because the Special Branch facilities within Scotland Yard in respect of counter-terrorism statistically form one of the larger deployments it is a convenient location for colleagues throughout the United Kingdom to act on a co-operative basis.

Q42 ***Chairman:*** It is a very complex web that you weave. I do not know about my colleagues, but it is quite difficult to try to find out where everyone links in. I do not know whether a map of how that works would help.
Mr Veness: We would be very pleased to supply that if that would be regarded as helpful. It will be illustrative for ourselves, I am sure!

Q43 ***Chairman:*** I know, whenever I have to look at anything complicated, having a map is just the easiest way. If members would be happy for that, we would be very grateful for that. How does it fit into Europol?
Mr Veness: It invites Europol to be an observer as part of the structure of the Police Working Group on Terrorism. I think your question is extremely well placed because there is a timely opportunity—I believe and I know colleagues would agree—to look at how many of these institutions might be more closely interleaved in relation to their operational effectiveness. I mention the fact that the Police Working Group on Terrorism historically has arisen from an earlier phase. I genuinely believe that there is a chance for us all to link in, particularly with the new invigorated role of the European Police Chiefs Task Force, which has moved on transparently since the initiatives of March of this year, post-Madrid. I think it would not be too critical an observer who would say there appears to be a degree of overlap here. I would point to the fact that the European police chiefs have a much broader agenda—drugs, illegal trafficking of human beings and other European cross-border issues of key strategic importance, as well as terrorism—whereas the Police Working Group on Terrorism has had this historic focus and has well matured systems of liaison, but of course there is the opportunity to work more closely, particularly with drugs liaison arrangements. Again, at the heart of your point, my Lord Chairman, I think there is an opportunity to explore a greater integration of the Police Working Group with the new and developing Europol structures.

Q44 ***Chairman:*** It would be good for me if you could put that as a sort of footnote what the police chefs do, and then the more strategic roles.
Mr Veness: The point that I had not addressed and that you raised in relation to how it actually deals with information is that primarily the working group operates on an intelligence-only basis, so its starting point will be to make inquiries, which might be quite mundane and routine, but nevertheless that gets the answer that deals with the imperative of taking action. Clearly what we are seeking to do is bring together information that reduces the risk of public harm. That is overwhelmingly what we are seeking to achieve. In an era when mass casualties would be the price that would be paid for not getting that right, that degree of rapid transmission is of course important. If one then moves into the slower time of using that information for court proceedings so it becomes evidence, then of course one would revert to the letters of request procedure by which the European and other nations will obtain that information more formally, but it does, of course, bring with it the practical advantage that you have already identified that the material you are seeking actually exists in France or Belgium as opposed to a speculative inquiry by way of letter of request.

Q45 ***Chairman:*** That is very helpful. It may be that members want to draw out a little more from that later. In the meantime, can I move on to my second question, which is about the European Council underlining the role of the European Police Chiefs Task Force in co-ordinating responses? Do you share the view that the role of the European Police Chiefs Task Force in co-ordinating their operational responses to terrorism is the best way forward?
Mr Veness: It is, I would suggest, an additional dimension and an additional network and source of energy which, if properly channelled, can be a valuable asset. I think the dimension that the European Police Chiefs Task Force brings is literally contained within its title, in that it is a senior body, which seeks to bring together decision-makers, leaders of European services. Of course, within the United Kingdom, we are not obliged because we have not got such an individual who could be described as the UK Police Chief. That role is performed by the Director General of the National Crime Squad on behalf of us all, but, in order that we are addressing the counter-terrorism dimension, one of my colleagues actually acts as the counter-terrorism deputy to the Director General of the National Crime Squad, so that we ensure that the United Kingdom has not only National Crime Squad business but also counter-terrorism as part of the agenda. I think the role of the Police Chiefs Task Force has clearly been advanced by events since Madrid because it is at the heart of the recommendations made by Justice and Home Affairs Council and the European Council. I think we are seeing a period, particularly under the

Dutch Presidency, where that is being given actual practical vigour and, in our view, a reasonable and achievable agenda of activities. The Dutch have delivered what they refer to as COSPOL, the Comprehensive Operational Strategic Policing Plan, which is to provide an agenda for the European Police Chiefs Task Force. We certainly, as the UK, are vigorously supporting the Dutch Presidency. We see one particular role as sharing with colleagues the benefit of hard-won experience here within the UK as to how operationally we respond to either the threat of terrorist incidents or the reality of terrorist incidents, because, sadly, the experience of dealing with bombs has been unhappily relatively commonplace here. That has led to an operation within the United Kingdom—and forgive me for all these labels—that is known as Operation Rainbow, and that is a spectrum of operational deployments that we can achieve. We are seeking to share that learning through the European Police Chiefs Task Force and the industry and the Dutch Presidency with our colleagues. I give that as one practical example of where that is being taken ahead at the strategic level.

Q46 ***Chairman:*** At the moment, it does not come under the Council's structures. Do you think it should do?
Mr Veness: I think it is an omission and an opportunity. It probably is inappropriate for me to comment about where that would appropriately fit in.

Q47 ***Chairman:*** Would it be helpful?
Mr Veness: There is a suggestion, given the seniority of the body, that something akin to the Article 36 strand of activity within the EU may be appropriate. Then I think there would be a need to align it with the administrative and strategic arrangements for Europol itself so that one had a clearer definition. No doubt that is a key role for Mr de Vries in his role as co-ordinator.

Q48 ***Chairman:*** We can ask him.
Mr Veness: It is a very real opportunity because there is a post-Madrid gap in relation to how the European Police Chiefs Task Force is integrated within the system, and how that fits together with the Europol activities.
Chairman: That will be a good question for next week when we go to Brussels and meet Mr de Vries. That is very helpful.

Q49 ***Earl of Caithness:*** The National Crime Squad has supported proposals to have small operational teams involving other EU countries, which is something that would follow on from improved Europol intelligence. Do you see this as a sensible way forward?
Mr Veness: I think there are very real practical benefits to be gained by the concept, but I think the concept needs to be applied in a way that it adds benefit rather than in any way it contributes to confusion. Perhaps I can illustrate that. The way that the joint investigative teams were emerging in the broader context of organised and serious crime, which is not terrorism, is that they were looking at longer-term problems such as illegal immigration, illegal smuggling of human beings and drugs issues, which were amenable to rather longer-term investment. In the context of dealing with terrorism incidents, the focus has actually been on material which is being developed which might lead to a terrorist bomb or some other form of incident, and there I think we probably need to think more broadly than Europe. Certainly, reflecting on the cases that have happened within the United Kingdom, even in this current year, which have yet to come to trial, although there was a European footprint, there also was the need to deal with a great many other jurisdictions much further afield. I think the joint investigative team idea has many benefits. Another dimension of it is when an incident occurs, for example the attacks on the Madrid trains, and the fact that that had immediate application to a range of other European countries. I think there is an opportunity to address the interests of those other countries and ensure that the inquiries are pursued expeditiously, which would be very much akin to a joint investigative team. What one does not want is that every time there is a bomb in Europe, 24 other nations all contribute individuals who may or may not have a role to play. I think my colleagues would agree we want rather more refined and bespoke arrangements. There is a third requirement that this concept could deliver, and again I use Madrid as the example. As soon as those bombs had happened, there was very clear enthusiasm on the part of everybody engaged in terrorism in Europe: what can we do to make the trains safer; how did this happen; where did they get the explosives; who was involved; and what does it tell us about European networks active in Europe? All of those questions need very urgent answers. It is almost not a joint investigative team but joint investigative communication that we need so that we have measures in place to ensure that our European colleagues are very promptly informed of those lessons. We would imagine, in the context of the counter-terrorism theme, developing this down those three broad avenues. In short, this is a valuable notion and one which needs taking ahead in a thoughtful and constructive way.

Q50 ***Earl of Caithness:*** Looking ahead and following up that answer, you have mentioned things like added benefit and being more closely integrated. Do

you see a need for an EU operational capacity? Are you differentiating between EU information, better and closer information, and then limited operational teams, or do you see it more as a big European operational capacity?
Mr Veness: I think if one added a label "European operational capacity" it is difficult to see what that concept or function would deliver that could not be achieved by what are relatively well-established mechanisms of counter-terrorism at the national level. My doubt would be whether one would always guarantee that when you went looking for that capability within a given location, even within Europe, you might find it. Certainly my personal priority would be to invest more heavily in national capability rather than to create, as it were, a specific European operational counter-terrorism capability, which I think would be difficult to fit in with the way that nationals regard counter-terrorism as part of their national security jurisdiction, and so there is not an overwhelming case that it would add benefit.

Q51 ***Earl of Caithness:*** Changing to a slightly different tack, on the evidence that ACPO and the Metropolitan Police gave us, there was this interesting phrase "within existing national structures and the constraints imposed by the nature of counter-terrorism intelligence data". What limits and constraints are you talking about? Can we lift the veil a little bit on that?
Mr Veness: On re-reading that sentence, I am conscious that it is not as happily expressed as it might be because it contains the words "it is difficult to see how co-operation could be improved on". I can think of a thousand ways to do that. If it conveys that sense of complacency, I apologise. That was not the intention. What we were seeking to convey in relation to existing national structures is precisely the point that I was alluding to in relation to capacity and capability. To be candid, there is a wide variation amongst even European nations in recognising the problem that post-9/11 terrorism confronts. Sadly, I think the cruel reality that we are seeing is that that understanding is coming about as a result of dire events rather than an intellectual process and a commitment to be fully engaged. I think the reality is that there is nowhere which we can exclude from the possibility of a terrorism attack being mounted, supported, recruited, provided with logistics, whatever, within the European theatre. We need to start with that understanding. I regret to say that is not yet fully developed. In terms of existing national structures, that is the point I am referring to: the political will based upon a clear understanding of the nature of the threat, a commitment to engage and to commit resources, and a commitment to address one's legal framework within that context.

Q52 ***Viscount Ullswater:*** As a supplementary to that, one of the first criteria that you identified in the role of the job that you do was that terrorism has now become global in the 37 months since 9/11. What we have been talking about are the sorts of European institutions. I wondered if you could just explain a little bit the role of Interpol and your work with Interpol, your connection with Interpol, because again you said that if there was an incident within the European Union, you did not want 24 people all gathering to try and deal with it. I think we have been told in written evidence that Interpol has what is called incident response teams, small numbers of people that can go and co-ordinate responses to events. Could you enlarge?
Mr Veness: On that latter point, it links back to what I was describing as the breadth of the strategic challenge all the way from when one has the first nugget of intelligence about a possible terrorist incident through the incident, if one is unable to stop it, and then dealing with it afterwards. I think the contribution of organisations such as Interpol is to bring together a range of national talents, skills and resources, which for example allow you to recover from that incident or to address the immediate crisis. We all ought to be actively supporting and engaging in that to make sure that that could happen rapidly when the need arises. Interpol clearly in a more general sense has the overwhelming advantage that it is the one global policing organisation. I think the encouraging dimension is the way, particularly under its present leadership, and indeed the contribution that has been made in terms of executive support from the United Kingdom, that Interpol has moved from a position of merely being an information exchange to developing particular contributions on a thematic basis. The one I would give by way of example is its work in relation to forged identity documents and in particular its aspirational global register in relation to passports and travel documents. That is immensely helpful. The disadvantage of course is that if you are moving on a truly global basis, then there may be some challenges in the extent to which you can be completely candid in respect of the sharing of intelligence that certain nations might regard as particularly sensitive. Is there an opportunity to drive ahead the agenda in relation to the greater role that Interpol could play? Yes, I think there is.

Q53 ***Baroness Gibson of Market Rasen:*** Could I ask a question about Europol at this stage? We are obviously very interested in how the institutional arrangements work. I wondered what you felt about that. Are you satisfied with the role of Europol and the role that is played in its fight against terrorism

and what you believe about its powers: does it need more or can it be effective as it is at the present time?
Mr Veness: I think even the most enthusiastic supporter would regard Europol as an evolutionary development. I think that is not being critical; it is being realistic. Seeking to move within a European policing cohesive body over the period of its development has inevitably been a challenge. To me, engaged in operational counter-terrorism within the United Kingdom, the one great advantage that Europol delivers immediately is that you have a range of European liaison officers from each of the constituent EU nations and they are actually there in one corridor or nearby; there is the ability to deal with a problem that might arise now with a European liaison officer from the United Kingdom being able to speak to somebody from Belgium and somebody from Sweden. Being able to address that issue is a very significant step forward. When one adds the number of different agencies that are now represented within Europol, and not only the police, in all their rich diversity within European states but also customs and immigration and in some cases security service officers, that gives a focal point, which I think is a very great operational asset. There are then the issues of the themes down which Europol can drive in order to assist. For example, after the Madrid bombs, it was the United Kingdom that engaged in a debate with Europol and said it would be a tremendous advantage to get together everybody who is responsible for transport and security both above ground and below ground in Europe to share what knowledge we have and what preventative measures we could take in relation to making rail transport safer. That was, I think, an excellent initiative taken by Europol in order to gather that degree of information. There is then the Counter-Terrorist Task Force, again reinvigorated after the Madrid bombings and contained in the declaration. We are vigorous supporters of that. I am proud to say that the United Kingdom is statistically the greatest contributor of information on that basis to Europol. The opportunity now falls, with the additional nations as part of the broader Europe, on development, training and demonstrating leadership as to how that can be brought together. I think some very real opportunities have arisen in terms of timing and the rather sad process of recent historical events and Europol is poised to make a valuable contribution.

Q54 ***Chairman:*** Can I go back to something that you said that I want to draw out. You said something like, "all Member States feel a real necessity to commit more resources to this and they all think the same and they feel strongly about it". That is not entirely my take on this. Are you satisfied that all Member States, even among the old Member States, are feeling equally anxious about getting this right?
Mr Veness: No. If I have conveyed that, then I have misled you.

Q55 ***Chairman:*** That certainly is not my feeling.
Mr Veness: To be candid, I think the problem of recognition of what this new dimension of threat means is patchily understood even within countries. One could say, purely from a counter-terrorist point of view, that one would hope there was a greater clarity of understanding of the situation. That was behind my comment to my Lord, that I think, if one looks at the record over recent months, indeed the last few years, understanding has actually arisen, sadly, when there has been a horrible incident rather than from some intellectual process of logic which has led people to do what is right, in our view, because that is the appropriate action. If I conveyed the impression that there is not scope for development within Europe, my view is very clear on that: we are nothing like where we need to be.
Chairman: That is enormously helpful because I have been quite concerned about one particular Member State that I would have expected to have been very focused on this but is not at all, to my way of thinking, and I will not name it. I am very grateful to you for clarifying that point.

Q56 ***Viscount Ullswater:*** So far we have talked about structures and co-operation but not to a great extent. Obviously what those structures do is exchange data. In your very helpful paper you noticed the difference between the data which is to be used partly for the judicial process and that which is to be used for intelligence purposes, and also of course there are the different legal views within the European Union as to the type of data that may be regarded as evidence, information and intelligence. Of course, we have that within our own structure within the United Kingdom too, just as a footnote. Do these various things hinder co-operation of data exchange?
Mr Veness: I think the candid answer to that would be "yes". Clearly, the information that is of the greatest imperative is that information which can save life or reduce immediate risk to the public. That probably means that our greatest investment should be in the intelligence channel, because that becomes intelligence which becomes information for action on which we can take practical steps. Of course, in an ideal world one would always want to move to a position where, in the vast majority of cases, one was mounting a prosecution and therefore one had the benefit of evidence which was admissible under the national rules applicable to that prosecution in order ideally that that would lead to the conviction of those responsible. Counter-terrorism, sadly, is a greyer

business than that. There are inevitably going to be occasions—one particularly senses that with the range of dangers that are now applicable in respect of new threats—when you need to move on actionable intelligence, and if that saves life, that is the outcome and one has reduced the risk. If one is in a position where it is not possible in those circumstances to mount a prosecution or indeed the compelling evidence one would seek to adduce is not available, that seems to me the right balance of judgment. The net result is that a terrorist attack has been prevented or disrupted. I think the key problem we have with the latter it that the issues of different legal structures are problems in relation to evidential admissibility. For example, when can a given national organisation begin to conduct an investigation and when can it mount surveillance? One sees a whole range of different, as it were, trigger points around the European Union that certainly, from a UK perspective, we would regard as difficult.

Q57 ***Viscount Ullswater:*** Do you feel then that perhaps there is some need for a common EU concept of admissibility of evidence and intelligence? Is it something that the European Union is there for? Is it a concept that the European Union itself should be doing or is it something that national governments should undertake on their own account?
Mr Veness: I think inevitably the initiative and the energy is going to be nationally led because of the understanding that this is a key element of each country's national security arrangements. Therefore, the imperative is to ensure that at a life-saving level, at the intelligence level, there is never the opportunity whereby a vital piece of information which would have saved a life in any country is reposing unaddressed and not being actioned. I think there is some benefit in work like the EU Plan of Acton, which has helpfully come out of the Madrid tragedy, and the concentration of effort by Justice and Home Affairs and the European Council. Achieving a common standard of admissibility of evidence, given the tension between common law systems, Napoleonic systems and others across Europe, would be ambitious in relation to the achievement, and perhaps it is not the absolute imperative if one is defining this mission as to save life.

Q58 ***Lord Dubs:*** I want to ask two questions. One is about information and the second is about intelligence, given what you have said about the importance of intelligence. This is about information: do you support the Commission's proposals for enhancing access to information by law enforcement authorities and the Swedish proposals for equivalent access to information? How will these contribute to the counter-terrorism effort?
Mr Veness: Having seen both of those, our sense is that, yes, of course, this is the right direction of travel. In many ways, we are not the owner of that debate, which is strategic and political. We recognise that. We are vigorously engaged in contributing to the discussion and so both the Commission's proposals and the Swedish proposals seem to us to be encouraging debate. Where we would want to add our imperative would be to relate to the previous issues about ensuring on an intelligence basis that nothing is being missed in relation to an exchange of a potential nugget of information that, as I mentioned, could reduce harm.

Q59 ***Lord Dubs:*** You have almost anticipated my next question. I think ACPO suggests that police forces should have access to national security intelligence. Would the intelligence agencies agree to that? In practical terms, how would you envisage facilitating the exchange of data between law enforcement and intelligence agencies?
Mr Veness: That may have arisen from Mr Tomkins.
Mr Tomkins: My Lord, I think we might have framed our evidence to the Committee rather poorly in this regard because, of course, we do have access to national security intelligence through bilateral contacts with the security services, and that is vertical contact. What we do not have are lateral contacts between special branches; that is, the security intelligence if any in the domain of special branches. We work on the basis of making requests to the Security Service at Thames House and the reply coming back but we do not necessarily have the means to interrogate the intelligence already, in our case, in our neighbouring force, Strathclyde. You may be aware that there is a national special branch intelligence system but that is something of a misnomer. It is not actually a national system. It sets national standards for the management of intelligence by the individual special branches. Indeed, Her Majesty's Inspectorate in England and Wales, when they conducted thematic inspections of special branches in 2003, which they entitled "The Need to Know", recommended that there be an integrated IT system for special branches developed to allow this sort of mutual interrogation because of the mobility of the subjects, of the intelligence, and so on. Given the nature of human procurement and the development of these projects, we might need a considerable time span, and so in Scotland, and we recognise fully this is a virtue of our scale, we are looking to create a parallel structure to that which we already have in criminal intelligence, the Scottish Intelligence Database, for special branches within Scotland, so that we would have some mutuality of insight within Scotland to address these issues. I am sorry if that initial evidence was misleading.

Q60 ***Chairman:*** Could I explore and draw out the question that we had last week but I think pertains to this as well and that is the difference between intelligence and information. Is either of you able to elaborate?
Mr Veness: Information is broad knowledge. In my view, particularly in the counter-terrorism context, intelligence is information which has gone through a process, an assessment and a judgment, and to which a value has been added, so it has an authority, it has a provenance, or it has a grading which takes it beyond mere news, as it were, if you can ally information with news on that basis. What I am looking for from intelligence is something about which I can form a view as to its value and what action can then be taken on the basis of it.

Q61 ***Chairman:*** Would you understand that all your EU partners share that view? Essentially, are we talking exactly the same language but do we all understand what we mean by that?
Mr Veness: The candid answer is clearly "no".

Q62 ***Viscount Ullswater:*** Could I ask a supplementary of Mr Tomkins? Did I get it wrong or are you saying that individual police forces' intelligence units cannot talk to each other on an IT basis?
Mr Tomkins: They cannot interrogate national security intelligence on an IT basis bilaterally between police forces. That is conducted through the Security Service, so the Security Service owns the intelligence and makes decisions on the nature of that intelligence and as to the propriety of sharing it with a particular special branch because of the actions they want taken.
Lord Dubs: Does that mean that if you want to get some intelligence which special branch in London has, you have to go to MI5 first to get it?

Q63 ***Chairman:*** Are you able to answer that?
Mr Veness: I think there is an issue around it. Special Branch acts in partnership with the Security Service in order to provide the counter-terrorist intelligence structures. I think one cannot look at this in purely police terms because that is only a part of the picture as to the way the United Kingdom addresses counter-terrorist intelligence. From my point of view, and I know it is true of Mr Tomkins and other police chiefs, we want the best possible intelligence hub that is going to be the most effective for the United Kingdom, and that clearly cannot be delivered by police forces; it must be delivered by a Security Service working in conjunction with other agencies which have the ability to reach and to receive material through liaison with international partners across the globe. In many ways, we act together with the Security Service in order to deliver counter-terrorism intelligence. On your specific point about whether we would expect to have unlimited access to that material, the answer is: no, because clearly the owners have got to respect the ability to get more information tomorrow and that relies on a very high degree of confidentiality. What I do expect is that the security services will work together in a confidential, effective and efficient way with the police forces around the United Kingdom. I think that is very close to being a UK success story, particularly when contrasted with a great many European jurisdictions. It would be a terrible shame if it was not because all of the experiences we have had of terrorism over the years have, in my view, produced a very effective and close partnership across the boundaries of security service work and police work.

Q64 ***Lord Avebury:*** It strikes me that before you start talking about exchange of intelligence between Member States, you do need to tackle what you hinted at: we do not have a common definition of intelligence. Should it not be a priority to try and get to the point where we know what each other means when we talk about intelligence and then we write down a definition which everybody then adopts?
Mr Veness: Yes, I think in practical terms what it means is passing of information today. The working assumption would be that which is actionable and useful in respect of countering terrorism but which is not going to be evidential could be categorised as intelligence. I agree with you that it would be neat to have an agreed form of words that was broadly understood across Europe, but does this act as a block this morning to people talking on an intelligence-only basis? I think probably not. The real problem is when one translates that information into evidence that one trusts is going to be admissible. I think that is probably a broader challenge.

Q65 ***Lord Avebury:*** Apart from the earlier definition you gave of what intelligence means, information that has been analysed and assessed so that people can draw conclusions from it, there is this other characteristic that it is not information which is going to be used in a court of law. That is another limiting condition which you apply to the definition of intelligence. With that definition, do you think there is a need to expand the exchange of intelligence between EU Member States?
Mr Veness: I think unequivocally there is. If the harm that we are seeking to prevent could be the mass murder of citizens within any European country, then if we were in any way complacent about the vigour or effectiveness with which intelligence is shared between nations, we would indeed be remiss. Yes, we must go on looking vigorously each day not

only for the intelligence being available but that it is gathered. That comes back to the point in relation to capability and capacity. My priority investment would be in ensuring that when we ask a particular nation whether they have that intelligence, then they actually engage in a process which will ensure that it is available.

Q66 ***Lord Avebury:*** Assuming it was available, what do you think are the main blockages and can you relate those to the Commission's proposals?
Mr Veness: I think the Commission's proposals would be a step forward in relation to liberating those issues, and indeed in the Swedish proposal I think they would probably operate rather more at the level where information is going to be shared in an overt sense, particularly for it to be taken forward to a court of law rather than acting as a blockage at the actionable intelligence end of the spectrum.

Q67 ***Lord Avebury:*** Could I ask you a question about what you said right at the start on progress not having been achieved in relation to the growth of support networks? You said, and I am not sure I have got your exact words, that radicalism contains extremism; in other words, there is a penumbra which may be very large in terms of its numbers and its spread and within which the kinds of behaviour we are looking at mature and are fostered. Do you think that the intelligence agencies are sufficiently conscious of this in the sense that they look at the intellectual and ideological background in which terrorism occurs? Do you, for instance, read the works of people like Qutb and Maududi and do other people in European countries research these ideological grandfathers of terrorism?
Mr Veness: Perhaps I could re-state what I was seeking to convey, my Lord. What I was suggesting is that one of the areas I would regard as somewhere we have not made sufficient progress in the last 37 months—but of course it is a much broader issue than that—is on the issues that cause the tensions that lead to radicalisation. I am not suggesting radicalisation is the problem but when radicalisation spawns extremism and extremism spawns violence which impacts upon innocent lives, I think that is the nub of the issue. In our judgment, what I can describe perhaps inelegantly as the support base is growing rather than diminishing because the causes of tension, not only in the sense of terrorism in its classical sense but the geographic, political and other issues which many will dub the root cause issues, are growing rather than diminishing. That is why I am suggesting that extremism is an absolutely key issue and one where I would suggest there is the opportunity for regions, in the sense of European and other regions, to contribute energy as well as what is done at the national level.

Q68 ***Lord Avebury:*** My question really was a more factual one than that as to whether or not you considered that on a European scale we need to collaborate in researching the ideological basis within which terrorism develops?
Mr Veness: Absolutely, and indeed there is some UK activity. I could point you towards where we are seeking, through the various mechanisms that I have described, to put extremism on the agenda so that we are addressing what I inelegantly described as the root causes, but I am using that in a generic sense. If we only address the consequences of terrorism, if we only deal with the bomb stage, we are going to find this problem getting larger over the years rather than diminishing, whereas I think we have a clear duty to seek to address this. It cannot only be a police and security service endeavour; this is a much broader social agenda.
Lord Avebury: I would be very interested if we could have that.
Chairman: That would be very helpful.

Q69 ***Earl of Caithness:*** I would like to follow up and take this a bit wider and ask the Assistant Commissioner if he could give his views on the global nature of this. We have been talking about Europe but you said right at the beginning that this is a global matter. How do you see not just the UK relating to the rest of the world but Europe relating to the rest of the world?
Mr Veness: Perhaps I could just explain what was behind my comments very briefly. I take the point completely that terrorism has been manifest in a range of locations across the planet for a great many years, notably with the current episode of terrorism from the end of the 1960s but there was a series of earlier phases. What is different, in our judgment, in relation to this dimension of international terrorism is that there is very obviously a cohesion which may not be tight but nevertheless a linkage in some form or another that has occurred, which has brought about an agenda which is unequivocally to cause the death of a great many people with, to some extent, dotted line linkages between those groupings. The most obvious cohesive factor would be the individuals who travelled to the borderlands of Pakistan and Afghanistan and went through training from a period in the mid-1960s up to October 2002 when Coalition action made that less likely in Afghanistan. What are dubbed the Afghan alumni then travelled to various corners of the globe to perpetuate the agenda and to take forward the methodology they had learnt in those camps. That is probably the easiest example. I think we have a

dimension of global impact that one can see in Indonesia, in Malaysia and throughout south-east Asia—and one can see it in the Middle East and across the span of the Maghreb—that represents a changed dimension of the threat of international terrorism. I think that is what I would describe as the new threshold, the novel dimension. Clearly, given that new challenge, there is an opportunity for regional institutions to make a vigorous contribution. If you do that with upwards of 200 nation states, it is going to be difficult to bring all that about, and I am in no way detracting from some of the excellent work that the United Nations has done, notably in Security Council resolutions, in respect of terrorist financing. I think there is a regional contribution that can be made which fits into that global challenge, if that is not a rather pretentious way of describing it.

Q70 ***Earl of Caithness:*** Can I get your comment on how those regional groups are now interlinking with regard to information and intelligence?
Mr Veness: Given that those bodies tend to be a support mechanism to national endeavours, I think the honest answer to that would be in a limited way at the moment. Where I think perhaps a more constructive and immediate contribution could be made would be back to the points of political will, commitment, problem understanding and developing capacity and capability. I think if one looks at the examples, notably in South East Asia, where there are things which have occurred in the last 37 months, development of regional training centres, development of expertise in dealing with bomb scenes that was not present and all that had been addressed on a regional basis, I would point to the practical contributions that could be made, perhaps in a less complex environment than information sharing.

Q71 ***Lord Avebury:*** I was going to ask on another matter, in relation to what ACPOS said about the inter-operability of EU databases, they see that as being a "mammoth task", by which I assume they mean it is not a practical proposal by the Commission. Both the National Crime Squad and NCIS see that there is a case for a centralised EU database for law enforcement purposes. Would you go along with that as an alternative, perhaps, to the inter-operability proposals and, if so, do you think there are intrinsic limits to the extent to which there can be inter-operability between the different agencies?
Mr Tomkins: Yes, my Lord, I think our scepticism was borne of our practical experience in Scotland and trying to get inter-operability on criminal intelligence between eight police forces, most of them quite small police forces, and therefore with small databases because of legacy systems and the nature of legacy systems that we have referred to in earlier evidence. Our experience was that we needed effectively to install a clean system, a new database, which would then operate on common shared protocols. If we extrapolate that to the position in England and Wales, where of course there are 43 forces which do not have a shared database, they do not have an equivalent to the Scottish intelligence database, and are reliant to some degree on bilateral arrangements with surrounding forces, groups of forces and so on, and then we extrapolate again to the complexity of the EU as a whole and the nature of legacy systems and the diversity of input criteria and so on, then I think that really informs our scepticism about being able to realise inter-operability protocols/criteria within the short term. I think, therefore, from our limited experience, we would say that it would probably be best to create a new database which would focus initially on the sharing of non contentious/non sensitive intelligence information such as identity records, finger prints and so on which could be accessed by constituent members of that database.

Q72 ***Lord Avebury:*** In some of the Scottish police forces, is there not a trend towards using open source operating systems and software? Would that help in maximising the ease of inter-operability?
Mr Tomkins: My Lord, if I understand you correctly, you mean open source intelligence?

Q73 ***Lord Avebury:*** No.
Mr Tomkins: Open sourced systems, web based system, yes, indeed, as long as the appropriate security—

Q74 ***Lord Avebury:*** —classification is adopted. Linux is its main operating system.
Mr Tomkins: Yes, but not for the Scottish intelligence database, it is a web browser based approach. I am going beyond my field of professional competence here, my Lord. My understanding is that the nature of the security operations for browser based type structures is becoming much more reliable and that might represent a more accessible and cheaper way forward and therefore a more timely way forward.

Q75 ***Lord Avebury:*** Can I ask both of you, do you think that the development of a common EU framework of data protection for the Third Pillar would be a good idea?
Mr Veness: Yes. Clearly it has advantages because one of the issues, particularly in relation to both intelligence and evidence runs into different interpretations of data protection criteria across the

European structures. I think, again, my Lord, the issue would be achievability at the political level.

Q76 ***Baroness Gibson of Market Rasen:*** I would like to explore a little bit about the G5 group which ACPOS has said is beneficial, I believe, and the Metropolitan Police/ACPO said that it does not undermine wider EU initiatives. I wonder if you could expand on this?
Mr Veness: I think G5 has got a valuable role to play. As you know it was here earlier in the summer, we were hosting the meetings. I had the opportunity to contribute at the working level with various operators from G5 which I think proved to be timely because literally we were in the weeks after March 11 and Madrid, and then also the Home Secretary generously invited the Director-General of the National Criminal Intelligence Service, the Director-General of the Security Service and myself representing ACPO to be part of the G5 deliberations when they met at the ministerial level. I was struck by the fact that here were five nations who were very seized of the problem, who had significant resources to contribute, and in many ways were inclined to act almost as a dynamo or focus of activity that it would be difficult to achieve in the broader, particularly now, 25 Member context. I presume it can never be perfect because there will be other countries who think there ought to be six or seven, and there are good cases to be made on that basis. My impression was that the ministers were keenly appreciative of wanting to be, as it were, a vanguard rather than a diversion. I sensed that there was a constructive role, particularly because of the timeliness of the fact that the action plan was now manifest, and here was something where a group of nations who were committed to driving that could achieve, I think, a valuable bringing together of various EU initiatives which, if we are honest, have been a bit spread about over recent times and to give some sense of direction.
Mr Tomkins: I think it would be hard to add to Mr Veness's eloquence on the subject other than to say from our perspective, really as has been said, it brings together the Member States with the core expertise in this field and it represents an engine for championing attention to the issue, as your Lordships have mentioned during the evidence to date.

Q77 ***Earl of Listowel:*** What contribution has the appointment of the EU counter-terrorism co-ordinator made? How do you think his role should develop now?
Mr Veness: Clearly it is in its early stages, an appointment made immediately after the Madrid events. Our view is that there is a very real opportunity and seen purely from a practical counter-terrorist point of view that opportunity would be to make sure that the various components of the EU machine are working together as effectively as they might and with a clear sense of direction and producing useful products and outcomes. I think the reality is that the energies of the EU in relation to counter-terrorism, and in the context of broader law enforcement issues, have produced a slightly untidy picture. We have a range of committees which have terrorism within their name. Also, we have a range of committees, initiatives and bodies which have some form of terrorism as part of what they do, either in the context of immigration or data protection. I sense that there is a very busy week for an EU co-ordinator in concentrating on that activity and bringing it together for useful benefit. To be frank, it is not for me to comment on Mr de Vries' working week but it seems in terms of EU practical counter-terrorism it should be very much focused on the internal workings of the EU and should not be adding a dimension of external representation because that is a function of the ministers of interior of Europe and should not be assuming what some might misinterpret as an ambassadorial role, again, I think that is the role of the ministers of interior. I think there is a real job to be done. In purely practical terms, the description that was provided immediately after March was a mite generic and I think there will be great benefit in tying down those terms of reference with a greater degree of precision.

Q78 ***Earl of Listowel:*** Are you suggesting then that his role should be to identify best practices, common standards and to put those forward as being helpful to making it all gel together?
Mr Veness: Precisely, my Lord, and I would add an audit of where counter terrorism is addressed within the various structures of the EU and ensuring that there was not duplication and there was a clear focus and direction to the way that the EU was supporting nationally delivered counter terrorism effort.

Q79 ***Earl of Listowel:*** That is very helpful indeed. If I might just come on and ask you about a particular point, that is how Eurojust fits into the picture you have been describing? A particular point we are taking up is that we have been learning that Eurojust's national representatives do not have the powers that one would really wish them to have. For instance, the legislative framework on which they are supposed to be operating, it has not been fully pushed through in all European states. Perhaps you could say a bit about that in relation to the coordinator's work?
Mr Veness: Yes, indeed. Clearly, Eurojust is operating in almost the most difficult end of this particular business, because it is seeking to grapple with the fact that for a whole range of other reasons

25 different legal systems are in play which were not created with counter terrorism cases in mind. I do not under-estimate the nature of the challenge. We welcome the fact that Eurojust like Europol, as it evolves, has begun to demonstrate that you can add value at the European level provided you define the contribution you are making and it is practicable, it is reasonable and is welcomed by the Member States. The very obvious gap was when you moved to translate that into court cases, where was not that same degree even of embryonic cohesion and, indeed, there was a greater opportunity for tension because of the differences between legal systems. I think the idea of Eurojust is extremely desirable, I think it is probably still in its network stage. It describes itself as a network and I think that is precisely where it is at the moment. There are other groupings that are dealing with information exchange amongst lawyers that are valuable. From our point of view, dealing with practical counter terrorism, it will be supporting prosecutors in relation to drawing together admissible evidence and the transmission of that evidence across European borders.

Q80 ***Chairman:*** Could I encourage you, Mr Veness, if you have not already read it, to read this Committee's report into Eurojust and the workings of Eurojust, which I would commend to you as the sort of definitive view of what Eurojust does. That might be helpful at some point.
Mr Veness: Yes indeed, thank you, I am grateful.

Q81 ***Earl of Listowel:*** How important is training in the developments of an EU wide counter terrorism capability? Perhaps before putting this question, I might just ask you if you have any further comments you would like to make about how existing European Union structures might be better streamlined in their counter terrorism work or do you feel you have already covered that particular point?
Mr Veness: I think in broad terms, if I was asked to reduce it to a nub, my Lord, it would be less of them, more effective and I think that is the agenda that beckons for the European coordinator.

Q82 ***Earl of Listowel:*** Thank you. Then to return to the question of training: how important do you think this is in the development of the EU wide counter terrorism capabilities and what role can CEPOL play?
Mr Veness: In operational terms, it is probably close to the top of the agenda. I would not demur from keeping extremism as the one trans-national area that deserves to be at the very top of everybody's agenda, but training is almost as critical because it is the engine by which we are going to deliver capability and capacity. Particularly when one looks at the movement from the eastern borders of Europe down into the Mediterranean of the problems that are linked with traditional drugs trafficking routes, traditional routes whereby people are smuggled and the extent to which they are exploited by terrorists as well, our ability at a European level to contribute through training to the effectiveness of operations and the ability of officers across a range of agencies to make counter terrorism more effective on the ground is enormously important. It is one where those western European nations in particular, who sadly have had more developed counter terrorist agendas, have got something meaningful to contribute. The development of CEPOL is welcome—it is good that its home is here in Hampshire and that it has its heart at Bramshill—and we want to encourage its development. I think we are in early days, we have got a small number of permanent staff, it is a virtual network. It has made good progress in 2004, I think 2005 beckons in terms of delivery of courses across a range of areas—and back to my strategic challenge—covering everything from intelligence all the way through to putting the city back together when some disaster has occurred. I think it is well placed to make that broad contribution.

Q83 ***Earl of Listowel:*** Has the training been targeted? Should it be at senior officers or at various levels throughout the EU? CEPOL concentrates on the senior officers, do you feel that more needs to be done at other levels?
Mr Veness: Yes I do. You have got to begin with an organisation understanding why it needs to be engaged in a particular problem, I think you have got to leave problem recognition to the bosses and then the rest of the pyramid hopefully will come into place. I think the importance of the training effort being across the span, as you suggest, is that one of our key judgments would be this dimension of terrorism is going to take years and years to contain, let alone to reverse the position that we occupy today. That being the case, I think collectively the leadership of British and European policing should be investing very heavily in our young men and women, in their analytical skills, in their understanding of the background of the problem, their ability to use language in a more effective way. That is in many ways an invaluable contribution because, sad to say, they will need those skills not only next week but in five years' time and in 10 years' time. I think a broad span of a rather more radical and innovative approach to training across the agencies is again a great opportunity.

Q84 ***Earl of Listowel:*** May I put one further question, if I may. Do you feel that the temporary exchange of senior officers is justifiable given the

obvious disadvantages to that and would you say exchanges of lower ranking officers should be encouraged? Is much of that taking place already?
Mr Veness: Yes, I think it is very valuable. The example I know best in recent times was after the tragic murder of our own defence attaché in Athens in June 2000. We worked very closely together with the Greek authorities doing precisely that, not only exchanging people who deal with recovery of bomb scene clues, dealing with fingerprint activity, dealing with analysis, all the way up to the senior officers who set the strategy and that proved to be a practical example of working together. It led to the benign outcome that a terrorist group that had defied detection for 25 years, N17, was, thanks to the energies of our Greek colleagues, successfully prosecuted. I could point to a recent practical example, including the UK, where that has worked across the span.

Q85 ***Chairman:*** If Members have no further questions I think that probably concludes our morning session with you. You mentioned learning in an effective way, I think people could have been no better placed than coming in here this morning and listening to both of you give your evidence to us. It has been the most informative morning that we have had and we have enjoyed it very much indeed. We have learned an enormous amount. We have been very fortunate to have you both giving your evidence. You have answered with great clarity and openness all of our questions. We are very grateful to you. Thank you again for coming.
Mr Veness: Thank you, my Lords, for your time.

WEDNESDAY 3 NOVEMBER 2004

Present	Avebury, L	Listowel, E
	Harris of Richmond, B (Chairman)	Ullswater, V
		Wright of Richmond, L

Memorandum by the Director General, Justice and Home Affairs Directorate General, European Commission

Justification

Does the fight against terrorism require much greater operational co-operation and freer exchange of data between law enforcement authorities (both national and EU)?

The terrorist attacks of 11/9 and 11/3 triggered wide-ranging actions at European level. Particular focus has been put on the need for better cooperation between all public authorities, sometimes in conjunction with relevant private sector actors. Priority is being given to implementing the 150 measures adopted by the European Council on 18 June in the form of a Counter Terrorism Action Plan. The Commission is fully engaged in this process.

At the Justice and Home Affairs Council meeting of 19 July, Commissioner Vitorino presented a Communication from the Commission entitled "Towards enhancing access to information by law enforcement agencies". This Communication responds to the request of the European Council of 26 March, which asked the Commission to bring forward proposals on exchanging personal information and on the use of passenger information for the purpose of combating terrorism, as well as provisions to enable national law enforcement agencies to access European information systems. In addition, the European Council instructed the Council to examine legislative measures to simplify the exchange of information and intelligence between the law enforcement authorities of the Member States.

These actions reflect the extent to which the fight against terrorism relies on wider, better and speedier information exchange to step up the law enforcement effort. But it is equally important to take full account of any potential impact on citizens' rights: a proper balance is required at all times between increased powers for police and other law enforcement authorities and protecting fundamental rights. In the Communication referred to above, the Commission announced that it will present proposals for data protection legislation to provide a single framework for the protection of personal data exchanged and processed by the law enforcement authorities. Informal consultations will be organised shortly by the Commission to sound out the needs and requirements of the stakeholders in this area.

Data Exchange

The Commission calls for the establishment of the principle of equivalent access to data by national law enforcement authorities in the EU. To what extent would this challenge fundamental legal and constitutional principles of Member States?

"Equivalent access" implies "under equivalent conditions"; in other words, in full respect of the safeguards which already apply to each national law enforcement authority. The nature of criminality, including terrorism means that national law enforcement authorities are increasingly obliged to cooperate to deliver results. They essentially have a joint responsibility to provide the EU and those who live in it with a high level of safety in an area of freedom, security and justice. The fact remains however, that the movement of persons within the Union is not yet matched by a similar ability to exercise law enforcement functions coherently across the Union through cooperation and joint working between national authorities. Since information is at the heart of any form of cooperation, it is only by improving access to information that the quality of cooperation will be improved as well.

The principle of equivalent right of access to data aims to ensure that better exchange of data does not have a negative impact on fundamental legal, or even constitutional principles.

3 November 2004

Wherever a Member State is of the opinion that access to certain information or databases is necessary for its police or customs authorities to carry out new tasks properly, it should also be recognised that law enforcement officials of other Member States exercising the same functions and fighting the same forms of crime have similar information needs. This means looking in detail at the various police functions and how and by whom they are carried out in each Member State, as well as at the conditions under which national officials access certain information. But, the Commission starts from the view that the fact that law enforcement officials fulfil equivalent functions and have similar information needs leads to the logical conclusion that they must be provided with access to the information that each Member State deems appropriate for the performance of these functions.

Furthermore, "equivalent" also means that the conditions for accessing certain information must be respected by all law enforcement officials (national or otherwise) who are entitled to access this information under the application of the right of access. These conditions may relate to data protection requirements, but also to the respect of data security and scrutiny rules. The Commission needs to have a clear picture of the conditions for access that Member States impose on their officials. Since law enforcement officials of other Member States would have access under exactly the same conditions as apply to national officials, it is clear that fundamental rights would be respected in full: the safeguards applicable in one Member State would apply to any access to that Member State's information by officers from other Member States.

The Commission calls for the interoperability of EU databases. What are the implications *of a facility for transferring data between databases? Is there a case for a centralised EU database for all law enforcement purposes?*

Discussions amongst Member States in the Council in 2002 highlighted that a large number of different databases were used by law enforcement agencies. At that stage no complete overview was available as concerns the various systems and the information they contained.

The Commission agreed with the need to develop an inventory of the various existing information systems in order to avoid overlaps and to ensure their compatibility.

An ad hoc group was mandated by the Article 36 Committee to carry out a study of the European information systems in Third Pillar areas. This ad hoc group consisted of the then Italian presidency, the Secretariat General of the Council, Europol, Eurojust, and the Commission and submitted its final report in May 2003 (Doc 8857/03 LIMITE JAI 118).

The report concluded that a limited overlap between the various systems existed and highlighted the absence of links between them. It identified three options to enhance synergies between the different systems:

(1) merge the different systems to become one European system;

(2) maintain the status quo and create new systems only according to clearly identified needs; and

(3) develop interoperability of the systems.

The Commission is in favour of the third option. It considers that although no need exists to set up an EU centralised database to improve the access to the information that is available, it is necessary to facilitate interoperability between data systems, ie national data bases will continue to exist and need to be inter-linked.

Data Protection

Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the third pillar, as advocated by the Commission?

The Commission is committed to striking the appropriate balance between legitimate law enforcement requirements and the protection of privacy, in conformity with the Treaties and with the Charter of Fundamental Rights of the European Union. High European standards for the protection of fundamental rights and freedoms of individuals, in particular their right to privacy, already exist. The Commission sees it as one of its key tasks to continue to ensure that these provisions are observed by both private processors of personal data and Member States.

At the same time, we cannot ignore the fact that our internal security environment has changed. Threats from international terrorism and crime have become one of the major security challenges for the European Union, in particular in the aftermath of the tragic events in Madrid on 11 March 2004. Therefore, the balance must be found between the requirements to fight terrorism and organised crime and to protect privacy.

3 November 2004

The recent Council Declaration on Terrorism of 25 March 2004 called for action on the collection and facilitation of the exchange of information. To deliver on this Declaration means creating the conditions for making relevant and necessary data and information accessible to EU law enforcement authorities, based on common standards, including data protection and data security provisions.

In addition, the EU has a duty to promote stability and security beyond our borders, in partnership with all relevant actors and partners. But here, as in our internal policies, gathering of personal data must be proportionate and balanced with the necessary safeguards.

The protection of personal data processed by police and judicial authorities must be effectively safeguarded by Union law and has to be based on the Schengen Implementing Agreement, the Europol Convention, the Eurojust Decision and the customs co-operation instruments which provide for specific data protection chapters with regard to personal data processed in the context of police and judicial cooperation in criminal matters. However over and above these specific regimes, general data protection rules do not yet exist for Third Pillar matters, as Directive 95/46/EC does not apply as such to processing of personal data for the purposes of Title VI of TEU.

Against this background the Commission is preparing a legislative proposal laying down standards for the protection of personal data within the Third Pillar.

Should there be common standards for the transfer of personal data from EU bodies and the Member States to third countries/bodies, including Interpol?

Common standards in this area could contribute to improving police and judicial cooperation in criminal matters between EU bodies and Member States on the one hand and third countries or bodies on the other hand. However, any proposals in this area could only be developed after a proper process of consultation with Member States' experts as well as with Europol and Eurojust.

The Role of the EU

Is there a need for an EU intelligence policy, as advocated by the Commission? To what extent can EU objectives be identified separate from those of the Member States?

The Commission does see a clear need to develop a criminal intelligence policy at EU level, especially to prevent terrorism. "Criminal intelligence" can be defined as "intelligence designated for use by law enforcement bodies", or more explicitly as "the information obtained, exploited and protected by investigation services and on which bases they take decisions and support criminal investigations".

An EU intelligence policy can help to focus and prioritise the efforts of the law enforcement communities of the Member States to combat criminality which poses a common threat in an area of freedom, security and justice**.** Criminality that stretches beyond the border of one Member State can only be tackled at European level. To be effective however, efforts undertaken in the Member States must be coordinated to address the same targets at the same moment, and strategic intelligence helps in that process of prioritisation.

EU strategic intelligence should allow each Member State to bring its strategic priorities for addressing terrorist threats in line with those of the other Member States.

The policy also needs to allow for the development of shared operational intelligence capacity, providing information on specific threats at an identified place and time. EU operational assessments should be formulated in such a manner as to be of operational use to the law enforcement community of each Member State concerned. In other words, the development of operational intelligence at EU level has to take full account of the specific law enforcement culture of each Member State.

How important is it for the EU to speak with one voice in the international arena in matters involving counter-terrorism co-operation?

The progressive establishment of an EU counter-terrorism policy needs to have a repercussion in international fora. This process needs to take account of the nature of this policy at a given moment.

Currently the EU is in the process of coordinating national and community policies that, taken together, are able to provide the EU with important counter-terrorism capabilities.

3 November 2004

The Treaties provide that common positions can be adopted by the Council to determine in a legally binding way the positions that EU Member States should take in fora in which they are members. It would certainly be politically desirable that this legal tool is used in such a way that internal EU policies are reflected in the external arena and that therefore the EU speaks with one voice.

Indeed, one of the challenges of current counter-terrorist action is the multitude of initiatives which exist in parallel in the different fora (UN Conventions, OSCE actions, G8 initiatives, as well as bilateral agreements). To reap the benefits of this action coordination is required, within the framework of the EU Treaties.

The UK recently hosted a summit of five Member States (G5) to examine measures to combat terrorism. Do moves of this kind prejudice EU wide initiatives?

The Commission fully acknowledges the importance of close cooperation between Member States to combat terrorism or other forms of serious crime within the area of freedom, security and justice.

The Commission is of the view that initiatives to improve and enhance law enforcement cooperation in the fight against serious crime and terrorism are best taken amongst all 25 Member States within the Council since the security of all citizens in the area of freedom, security and justice is a matter of common concern.

Only when serious analysis has shown that it is not possible to reach agreement between 25 Member States, should the use of the instrument of enhanced cooperation as laid down in the Treaties be explored. Currently a large number of initiatives are on the table of the Council that to a greater or lesser extent contribute to the capabilities of the Union to combat terrorism. A determined effort is required to bring these initiatives to fruition, and the Commission would like to see all Member States take part in these measures.

Institutional Arrangements

What is the added value of the post of EU Counter-terrorism Coordinator? What should his role be?

The Commission has developed effective cooperation with EU Counter terrorism Coordinator, Mr de Vries. The EU Counter Terrorism Coordinator has contributed to efforts to improve the fight against terrorism by producing papers for discussion in the Council in the fields of:

(1) legislative instruments to fight terrorism: monitoring of the implementation;

(2) the working structures of the Council in terrorism matters; and

(3) provisional findings on the two peer evaluation exercises (national anti-terrorist arrangements and exchange of information Europol/MS).

The Commission believes that one of the main contributions which Mr de Vries could bring to this work would be to continue to tackle the extremely unsatisfactory rate of formal adoption and of implementation of adopted measures by the Member States. In this regard, Mr de Vries has stated that he shares the Commission's concerns and has vigorously denounced this state of affairs in Council. It is highly regrettable that given the absence of the possibility to take infringement proceedings under the Third Pillar, many Member States continue to systematically fail to meet their obligations in areas which are of paramount importance for the internal security of the Union.

Secondly, Mr De Vries could contribute to further improving the Council working structures on terrorism.

What changes are called for in the EU's institutional arrangements (including Europol, the European Chiefs of Police Task Force (ECPTF) and the Terrorism Working Group) in order to combat terrorism more effectively?

Several Council or other EU structures are currently dealing with aspects of the fight against terrorism with little overall coordination at EU level. There is a risk of a negative development in which:

(i) intelligence services by way of the Terrorism Working Group submit information to the Situation Centre or SITCEN (ie the EU Situation Centre set up within the Council and assembling Members of External Security services);

(ii) police/criminal intelligence services report to EUROPOL; and

(iii) national operational assessments are given to national police authorities with no common operational platform. The Commission considers that it is fundamental to ensure close and effective communication between the above-mentioned structures.

3 November 2004

The European Chiefs of Police Task Force (ECPTF) was created by the Tampere European Council. At present it works outside Council structures and aims at co-ordinating operational activity at cross border level on serious crime such as terrorism. Discussion is under way in Council on increasing the operational capacity of the ECPTF and integrating it into the Council structures. The Commission welcomes integrating the ECPTF within the Union decision-making framework with the operational support of EUROPOL.

Under the aegis of EUROPOL, the Member States' Criminal Intelligence communities should assemble national strategic and operational assessments and present the resulting EU strategic assessment to Coreper and the JHA Council and the EU operational assessment to the ECPTF to be handed down to the national operational levels. Europol should contribute with all intelligence it has available. The intelligence could be collated to produce EU strategic assessments twice a year, and EU operational assessments every month. The EU strategic assessments would allow the Council to set law enforcement priorities. The ECPTF should then hand down the operational assessments to the operational levels within national law enforcement communities. This approach should lead to a situation where strategic assessments are readily available to the decision makers in order to revise law enforcement priorities as often as necessary. Operational assessments would be made available to the ECPTF providing the law enforcement community with the best available tactical knowledge to prevent or combat the threat of terrorism.

Operational modalities and channels of communication should be found between Europol, SITCEN and the ECPTF.

What contributions can EU level training and in particular the EU Police College (CEPOL) make?

Over the last three years, CEPOL has already made an important contribution to European police training. The Commission is pleased that the legal personality and a permanent seat have now been resolved with two Council decisions adopted on 26 July 2004. The Commission has now put forward (1 October 2004) a proposal for a Council Decision aiming at establishing CEPOL as an EU body and entitling it to funding from the EU budget.

Out of the 70 training sessions already organized by CEPOL, some **"flagship" courses** have been organized on **Anti-terrorism**. The objectives of the courses were to analyse the phenomena of international terrorism and its wider international relationships with other phenomena, and to estimate the potential threat and discuss prevention and reduction strategies. The training sessions dealing with **knowledge of the National Police Systems** also touch upon the subject of investigation of special crime and terrorism. Subjects such as terrorism are also dealt with in courses organized in the framework of the Community Assistance for Reconstruction Development and Stabilisation (CARDS) and the Euro-Mediterranean Partnership (MEDA) programme which include third countries such as Croatia for CARDS and Turkey and Morocco for MEDA.

CEPOL's Annual Programme 2003 reflected the priorities set by the Council. Two specific courses were delivered in relation to anti-terrorism, dealing with **Management of Information** and **detection of falsified documents.**

The objective of the course **Anti-terrorism and Management of Information** was that delegates should be able to analyse the phenomena of international, especially religiously motivated, terrorism and its international ramifications, to assess the potential threat and to discuss preventive and repressive control strategies.

The objectives of the course **Anti-terrorism: detection of falsified documents** were to allow senior officers to develop their capacity to detect forged and falsified identity documents, by using standard strategic principles and detection techniques, and to transfer the necessary knowledge about detection techniques to the trainers who are active in the field of anti-terrorism.

Seminars and Courses on Anti-terrorism remain an urgent and continuing need. The added-value of promoting co-operation between the EU Member States and developing language skills among participants should not be underestimated. In the programmes for 2004 and 2005, CEPOL's Annual Programme Committee has duly taken into consideration the request from the Chiefs of Police Task Force for CEPOL to develop training modules in the field of information management, related to the fight against terrorism and more recently, their request for additional courses for Joint Investigation Teams.

The flagship course on anti-terrorism aims to analyse the phenomena of international terrorism and its wider international connections, estimate the potential threat and discuss prevention and reduction strategies and assist in the detection of forged and falsified identification documents.

7 October 2004

3 November 2004

Examination of Witnesses

Witnesseses: MR JONATHAN FAULL, Director-General, and MR JOAQUIM NUNES DE ALMEIDA, Head of Unit, Fight Against Terrorism, Directorate-General Justice and Home Affairs, European Commission, examined.

Q86 ***Chairman:*** Thank you very much indeed for inviting us to come to talk to you. We are very interested in what you have sent us already and I would like to thank you very much indeed for that. Could I introduce my team: on my left are Lord Wright; Valsamis Mitsilegas, our legal assistant; then Tony Rawsthorne, our clerk; John Abbott, our specialist adviser; Lord Avebury; and the Earl of Listowel. We are waiting for Lord Ullswater, who we hope will join us fairly shortly. If I could start with the questioning and ask, first of all, about the problems of exchanging data at national level and what you understand to be "equivalent access". What is meant by that?
Mr Faull: Equivalent access essentially means that a Member State's law enforcement authority should have access to information in another Member State where that other Member State's law enforcement authority would have access to it with all the safeguards already in place in the Member State in which the information is held being complied with.

Q87 ***Chairman:*** Thank you. For the record, as you will understand, when our report comes out it is important that we have your understanding of that. You refer to the potential impact of the application of the principle of equivalent access on fundamental legal and constitutional principles in Member States. Do you have any examples of that?
Mr Faull: At the moment national law enforcement authorities have a right of access to information within their territory in accordance with the law and under the supervision of the supervisory body set up in that country. When seeking access to information in another Member State, we have to make sure that the information is to be used in ways which do not infringe the fundamental principles of law which are common to all of our constitutional traditions, particularly the protection of fundamental rights, such as the right to privacy. I intended to highlight in my written evidence that in our initiative to establish a right of equivalent access to information across Member States, it must be made clear that those fundamental rights are respected. The Commission has announced that it will table legislation on the protection of the exchange of personal data under what we call the Third Pillar of the European Union, and we look forward to a meeting with experts of Member States on this on 22 November—if that meeting is still on.
Mr Nunes de Almeida: Yes, it is.
Mr Faull: Okay. At this stage we are compiling information about the protections and safeguards which are already in place in the Member States. There will be three meetings of experts to consider this: law enforcement experts on 9–10 November; the Civil Liberties Committee of the European Parliament and non-governmental organisations active in the fundamental rights' area will meet on 23 November; and we will meet the national data protection authorities—the supervisory bodies—on 14 December. *(Lord Ullswater entered the room)* We will also launch a study on the conditions and provisions on the monitoring of respect for fundamental rights. That study will be launched before the end of this year. Our reference to fundamental legal and constitutional principles was intended to cover the various measures for the protection of fundamental rights in the Member States, both national and European, and we need to find ways of making sure that this right of equivalent access does not infringe them in any way.

Q88 ***Lord Avebury:*** As a result of these studies that you mention, will the legislation that is finally tabled be a superset of all the conditions which are imposed on access to information in every Member State?
Mr Faull: It is too early to tell precisely what will be needed. I think probably not. I think we will find that in the Member States already under the umbrella of the European Convention on Human Rights there are rather similar protections already in place for this sort of information. The very purpose of this principle of equivalent access is that we take each Member State's system as it is and, where in a national system access would be granted, it then should be granted to the others; where it would not, it should not. That does not mean that it may not be necessary to have some minimum level of agreed standard of protection, but we will not know that until we have a clearer idea of precisely what in the 25 Member States is already happening. I talked about the Third Pillar, which is the intergovernmental Justice and Home Affairs pillar of the Union. In the First Pillar, the more traditional European Community pillar, we already have a data protection system under a Council Directive, which has established a set of common rules, and there are supervisors in each Member State, data protection authorities, which are responsible for enforcing and giving opinions, and they come together in a committee at European level and provide us with advice and opinions as well.

Q89 ***Chairman:*** We were told by one of our witnesses that there was concern about the threat to sources. Some preferred bilateral exchanges in terrorism. What is your view?

Mr Faull: Obviously information which is provided by sources or as a result of methods which Member States wish to keep secret, should not, through information becoming available to others, inadvertently or indirectly reveal a secret source or a particular method of discovery. We would have to make sure that safeguards for that particular issue, obviously of great importance to the intelligence communities, are either already present in the 25 Member States' national systems, or, if not, this could be an example of where we would have to introduce some common European definition and provision.

Q90 ***Chairman:*** And you think that would be almost certainly a necessity.
Mr Faull: It is likely to be, because I do not think that across all 25 Member States there are the same traditions of "fact-finding" in this particular area.

Q91 ***Chairman:*** Which country's legal system will regulate the use of data accessed by the foreign police officer?
Mr Nunes de Almeida: That is something we are trying to find out in the stock-taking exercise. It is something we are to find out yet in the meeting with the experts that Mr Faull has spoken to.
Mr Faull: It is obviously a very crucial issue and one which will require a great deal of attention. It is too early for us to tell at this stage what the best or most appropriate solution is. It is obviously something we will have to discuss with Member States and others.

Q92 ***Chairman:*** Thank you very much. That is extremely helpful. Could I move on then to state sovereignty and equivalent access. In the area of police and criminal law, would not equivalent access threaten state sovereignty, especially if it extended to any information held by the police? Should that be limited to information related to terrorism?
Mr Faull: There are two questions there really: whether we should limit this initiative to terrorism alone and the question of sovereignty. To start on the sovereignty point, it seems to us that sovereignty is respected where each State determines autonomously the conditions under which information held within its territory may be made available to others, whether that be under existing national law or under EU legislation. That seems to me to be the proper exercise of sovereignty: "I, the sovereign, decide under what conditions information in my territory should be made available to others." Our fundamental idea is to say that, where information in respect of that rule would be made available to an authority within the territory then an equivalent authority in other Member States should have access on the same conditions and in compliance with the same rules.

Q93 ***Chairman:*** Is that the same as the "pooling" of it—bringing all together?
Mr Faull: No, it is not the same. It is not the same as saying all 25 Member States feed all the information they have into one computer in Brussels and then we will clear it out to everybody else. That is not the system we are envisaging. The system we are envisaging is one where law enforcement authorities in other Member States for certain defined purposes—and that is the second question to which I will come—should have access to information where the national law enforcement authority would have access to that information. Now: terrorism alone or terrorism plus other types of serious crime? It seems to us it would be difficult practically and in organisational terms to limit information to terrorism alone. In the first place, it is difficult to determine exactly what information is necessary in order to prevent or combat terrorism. The information may be trivial at first sight; it may be very complex and sophisticated at first sight. A car theft may have a link to terrorism and it may not. Our experience is that, more and more, organised crime in other fields and terrorism are linked.

Q94 ***Chairman:*** Certainly that would be the evidence that we have found in the past when we have dealt with this. Is the "principle of the availability of data" the same as equivalent access?
Mr Faull: "Availability" is the Dutch notion—and I rather hope it is the same as the right of equivalent access. This is the term which they are hoping to introduce into the new multi-annual programme to be known as the Hague Programme which we hope the European Council will adopt on Friday. The Dutch believe—and this is really a question for them more than for me—that where relevant information is available within the Union, the law enforcement authorities of one of the Member States that need the information should be able to obtain it. Our notion of equivalent access, it seems to me, is slightly more operational than that. It gives operational effect to that notion by adding the notion of equivalence, which means that the national rules on access would have to be complied with in each case; otherwise, you would need a set of European rules on safeguards, which would take a very long time to negotiate and to give effect to. It is much better—and this is, after all, how the European Union has developed in so many fields—to take the national situations as they are and use them as the basis for the legislative measure that says that, once something is allowed in a country, it should in principle be allowed everywhere. It is, after all, at the heart of the free movement of goods in the European Union: if a product is legally marketed in one country, nothing should be put in the way of its being marketed in other countries. The Home Licensing Principle for

banking is another example. If a bank is licensed to operate in one Member State, it should be able to operate in all of them, because you trust the regulatory systems of each of the Member States. If you have reason not to consider that all of them are of acceptable quality then you may need some minimal degree of harmonisation. We are essentially doing the same thing here. We are saying: "Member States have rules on access by law enforcement authorities to data. We will accept them as they are. If some of them, on analysis, turn out to be inadequate, we can establish a common minimum, but the basis should be that the national rules apply, and, where the national rules would authorise the law enforcement authority in that country to have access to information, the law enforcement authorities of other countries should have access on the same basis."

Q95 ***Chairman:*** Do you think that every other Member State has that understanding of what the phrase means? It is a language thing, is it not?
Mr Faull: It is. Well, language things are pretty important in the European Union: we have 20 languages.

Q96 ***Chairman:*** Is anything being done to ensure that you all understand—
Mr Faull: Yes. Absolutely. This was all being discussed in various meetings. The Dutch draft programme has been through two meetings of the Justice and Home Affairs Council; it was yesterday in the General Affairs and External Relations Council; the ambassadors in Coreper have been over it with a fine-tooth comb—and what I have said, I think, is the general understanding. Availability is, as I said, slightly less operational and precise than our notion of equivalent access, but our notion is one which is up for debate. Availability leaves open, of course, the conditions under which availability should be granted, and that is a matter for further debate and discussion.

Q97 ***Chairman:*** Thank you. We have talked about the Hague Programme, could we move on to the Swedish proposal for simplifying the exchange of information and intelligence between law enforcement authorities. How does that relate to the Commission's proposals?
Mr Faull: Our understanding is that the Swedish initiative is designed to improve sharing of information in the short term. Our proposal, on the establishment of a right of equivalent access, is seen by delegations in the relevant Council working group (known as the multi-disciplinary group) as a longer-term project which will provide for a wider sharing of information between law enforcement authorities of the Member States in the future. The Swedish initiative has four main ideas: to allow direct requests and answers for information between law enforcement authorities; to impose an obligation to respond to those requests; to set a deadline for certain types of information of 12 hours; and not to apply to requests conditions more stringent than those that would apply to a national request—which is the beginning, I think, of the same idea as the one we are pursuing. We are considering at the moment how to respond to the Swedish initiative—the Commission always gives a written opinion on national initiatives of this sort. We have not finalised our work on that yet but we are considering the idea that it might be more expedient to bring about the improvements the Swedish initiative is designed to achieve by amending rules under the Schengen system; to be more precise, articles 39 and 46. We will have to wait and see how work proceeds on the Swedish initiative. As I said, we have not yet produced our own opinion on it and work in the Member States and the Council is only just beginning.
Lord Wright of Richmond: Mr Faull, before we move to interoperability—and I am not sure that I can pronounce that word.
Chairman: That was perfect!

Q98 ***Lord Wright of Richmond:*** Is there much distinction between the ways in which different members of the European Union provide intelligence? Are some members providing raw intelligence, others only analysis and assessments? Is there much difference between them?
Mr Faull: I am not sure I quite understand: providing to whom?

Q99 ***Lord Wright of Richmond:*** To you and your colleagues.
Mr Faull: No, there is not a great deal of difference. The provision of raw intelligence information is extremely limited. That would be very much the exception, because of all the dangers of revealing sources and methods about which Member States are rightly very sensitive. There is a great deal—and a growing amount—of discussion of more processed intelligence and what people think it means, but occasionally you will find that Member States picking up a piece of information, which to them might be meaningless or apparently trivial, will provide it to others because it might be a piece in a jigsaw to them, working on some other type of analysis.

Q100 ***Lord Wright of Richmond:*** Your very helpful written evidence reflects the need to enhance the interoperability of the EU databases. Could you tell us a little more about what is meant by that. What are the main problems in data sharing at the moment which this enhancement is designed to cope with?

Mr Faull: Interoperability . . . I hope it is an English word, by the way, we probably invented it from the French or Italian or Portuguese or something.

Q101 ***Lord Wright of Richmond:*** I am sure it is, but it is a rather long one.
Mr Faull: A terribly long one! It means the ability of two or more systems to exchange information between themselves and then to process that information further in accordance with their own systems. It requires common technical standards obviously: the computers have to talk to each other, which requires common definitions of data and structures. Why do we need it? We think there is a practical operational need. Very simply, a stolen firearm, for example, might be recorded in two different data systems under different definitions, and then somebody using system A, asking the question of somebody using system B, would not get the correct answer. It is, initially, a technical problem. It is to make sure that computer databases can speak to each other, can interrogate each other, and that people familiar with one system can find, use and process further information held in a second system.

Q102 ***Lord Avebury:*** Could I interrupt you there. On your example of the firearm, in the two separate systems a person accessing data which may not be identical, is that not a question of standards rather than interoperability? Because, if you have methods for recording stolen firearms, for example, and those are universal in the States concerned, then there will be no danger that one database will have a different description of that firearm from another, and the person accessing that information on the two different databases would get the same result. It is not a question of whether or not the information is readily transferred between one database and another, is it?
Mr Faull: No, it means that if . . . I am trying to think of an example. If a police force in country A wants to find out whether a suspect is licensed to hold a firearm, within the national system that is, I imagine, in real time a very simple thing to do. If you then want to find out, "Ah, but has this person been licensed to hold a firearm in other Member States?" and through your own computer system you just want to press another button and say, "Check all the others" or "another", in order for that to be a successful operation, both systems need to share a definition of what is a firearm and what is not. It is purely technical—plus, of course, the two computer systems being able to link into each other rather than someone having to make a phone call (or 24) to get someone else at the other end to do it.

Q103 ***Lord Wright of Richmond:*** Does that mean adjusting existing systems or actually going for completely new contracts? We have noticed that some contract under the Schengen Information System was signed last week. Is this a way of achieving interoperability?
Mr Faull: If you are designing a system from scratch, as we are with the second generation of the Schengen and Visa Information Systems, it makes sense, as we have done, to provide the capability within the system. But there are already vast databases which were designed quite separately from each other where questions of interoperability have to be addressed now, and where the questions of definition arise.

Q104 ***Chairman:*** What happens if it is outside the EU? What sort of global problems are there? Where does Interpol sit?
Mr Faull: Interpol, of course, has international range and we should use it to the full. We have established—and of course national police forces as well—very good relations with Interpol, and Europol has its own good relations with Interpol. At the moment we are not considering—apart from one specific area which I will come to in a minute—opening up systems to the rest of the world or vice-versa on a reciprocal basis. It is hard enough to make progress among our 25 countries in this area. This is already quite an ambitious task. One area where we have taken the initiative with Interpol, in agreement with the Americans, is to provide information on stolen and lost passports, where we now, with the Americans—and increasingly, I hope, many others in the world—provide Interpol with information about passports which are stolen or lost, either already issued ones, or, even worse, blank ones, so that immigration authorities and police forces can check very quickly on an Interpol database whether a passport presented was really issued to the person presenting it.

Q105 ***Chairman:*** The firearms example you gave us seems to be about Member States rather than EU databases like SIS.
Mr Faull: Yes, that is right. We do not have a European firearms database. I am not suggesting we should have one. Wherever possible, in principle, we do not want to have databases of our own; we just want to get national databases operating together—just as, on the law enforcement issues we were discussing earlier, we want to find a way for the law enforcement authorities in one country to have access to information in another where their counterparts in that country would do so. The last thing we need is a centralised system here, with the Commission or somebody else acting as a clearing house. In some areas, though, we do need Community-wide or at least Schengen-wide database systems. We have the

Schengen Information System, we have the Visa Information System, and we have the Eurodac system for asylum seekers. Another question—an extremely important and sensitive question—is the extent to which those EU-run databases should be made interoperable with each other.

Q106 ***Chairman:*** Would interoperability apply to Member States' databases
Mr Faull: Yes. If agreed, it could certainly do so.
Mr Nunes de Almeida: The danger being that each database is created according to its own specific technical standards and then they are unable to speak to each other. So interoperability is a purely technical concept, and then comes the political question: if you actually wish to talk to each other or not. But interoperability simply means that you design the 25 different databases nationally in a way that allows, if the political will is there, for them to talk to each other.
Chairman: I am straying into Lord Wright's further questioning.

Q107 ***Lord Wright of Richmond:*** No, you have really answered all the questions I wanted to ask, except for one that is here on the hymn sheet; that is, is there a case for changing the structure of the Schengen Information System to address terrorism? Is that contract, to which I have already referred, of last week an attempt to change the structure?
Mr Faull: No, not really. We believe that the SIS as it is today is already a useful instrument in the fight against terrorism. It allows alerts on wanted persons for arrest to be introduced to the system and also allows for the alert system to cover persons who should be the subject of discreet surveillance or subjected to specific checks and persons who should be refused entry because they have committed or are believed to intend to commit serious criminal offences. So we think that the SIS, as it stands today, without any need for restructuring, can play and, indeed, does play an important role in the collection and dissemination of information for counter-terrorism purposes. The second generation, which, as I said, is designed to include interoperability features from the beginning, would not change its fundamental purpose, which is that it enables, within seconds, information to be provided to those who need it on whether persons should be allowed access to the Schengen territory and thereafter free movement within the Schengen territory, or not.

Q108 ***Viscount Ullswater:*** You describe interoperability as being a technical problem, but in order for that information to be sought by the various Member States they have got to have agreed, have they not, on equivalent access? Does one come before the other? Can they be developed at the same time? Or are there some sort of impediments which stop interoperability because you have not agreed on the sort of trust that is required for equivalent access amongst the 25 members?
Mr Faull: Absolutely. The key to interoperability is the "ability" bit of it; that is to say that it creates a possibility, a function. The political decision is whether to use it or not and what conditions should be set on its use. That is very much a matter of political debate and, ultimately, for political decision: Which types of information should be shared with other authorities, for what purpose, for how long and so on? Already, within Member States, within each country, there are, for perfectly good reasons, restrictions on the use to which information collected for a specific purpose can be put. People are rightly sensitive about that and about sharing that information beyond the national borders with the rest of the European Union. That requires political decision on a case-by-case basis. The interoperability just makes it possible, if the political decision is taken to create a right of equivalent access in the specific case, to do it in the most sensible and convenient way possible.
Chairman: Thank you very much. Could we move on now to areas of data protection and I would ask Lord Avebury to ask questions on that.

Q109 ***Lord Avebury:*** You were speaking earlier on about various things which have to happen before the legislation is introduced. Is it possible that you could let us have a bar chart showing us the time scales of these various developments leading up to the tabling of the Commission's legislation?
Mr Faull: With pleasure. We will certainly try to do that. There will be a certain amount of uncertainty about precise timetabling because some of it is out of our control, but we will provide you with that.

Q110 ***Lord Avebury:*** Thank you. Could we talk about the coordination of the various EU joint supervisory bodies. First of all, does the Commission envisage a greater role for the European Data Protection Supervisor in overseeing data exchange for Third Pillar matters in the future?
Mr Faull: In a way I am afraid it is too early to give a precise answer to that because a lot more work will be needed; in particular, of course, consultation and discussion with the data protection bodies concerned, with the data protection supervisory bodies. We are starting those discussions now. Obviously, it seems to us, the co-ordination of the supervisory bodies should be as effective and transparent as possible and we should encourage them to work together.

Q111 ***Lord Avebury:*** There is a proliferation of these bodies, is there not? The co-ordination responsibility must become very burdensome, I would imagine. Do you think there is scope in the discussions between the joint supervisory bodies for simplifying the whole system of supervision or not?
Mr Faull: There may well be. We will certainly strive for simplification. I cannot say today precisely how much consolidation and simplification will be possible. These are complicated areas and they have tended to lead, perhaps unnecessarily, to a certain proliferation, as you say, and specialisation. We would certainly hope to have the simplest system possible, with joint supervisory bodies as limited in number as possible and working as closely together as possible, with co-ordination being as light as necessary. All of that is easy to say, hard to bring about in practice, but that would certainly be our guiding principle.

Q112 ***Lord Avebury:*** The joint supervisory bodies highlighted in their evidence the fact that national data protection authorities have different competencies in the field of law enforcement. Do you think there is a need for national data protection authorities to have equivalent powers in this area? Is there a case for greater co-ordination between the national data protection authorities?
Mr Faull: Subsidiarity, of course, has an important role to play here. The precise powers of the national data protection authorities are obviously a matter of concern to us in respect of their possible impact on police and judicial cooperation as provided for in the Treaty. We will certainly be looking at that. We do not want to go too far in consideration of the national bodies' powers because some of those powers are irrelevant really for the European context. They have a very important role to play in the purely national context and we do not want to get in their way. Again, in this consultation process which we are starting, we will be very attentive to the borderline between what is necessary by way of common standards and procedures for the proper functioning of the Union's work in this area and what can be left with national differences for operation on the purely national level. It is essentially the same, I am afraid, as the answer I gave you on proliferation or consolidation. Obviously this is something we would like to see. We will have to see in practice, however, how far we can go.

Q113 ***Lord Avebury:*** Is there a mechanism for consulting with the 25 national data protection authorities? What is the mechanism for that?
Mr Faull: There is. They come together in a committee in Brussels and then there are all sorts of informal opportunities. I am sure than in an area of such importance to them as this they will not hesitate to make their views very clear and we will certainly be seeking their views.

Q114 ***Lord Avebury:*** In your legislation or elsewhere are you going to specify under what conditions the transfer of Third Pillar data to third countries could take place?
Mr Faull: The data protection legislation for the Third Pillar that we are preparing should cover that issue but only in so far as is necessary for the improvement of police and judicial co-operation under title 6 of the EU Treaty. From a political point of view, it seems to us that the Union should act together where issues of internal security and police and judicial co-operation across the Union are concerned. In the situation in which exchange of information across the Union is being advocated, it would be hard to understand that rules on transmission of information to a foreign country, to a third country, should be different from one Member State to another. It is therefore arguable that co-operation between police and judicial authorities of Member States would be hampered by practices which diverged, at least to a significant degree, in relations with foreign countries. The exact conditions to be worked out for transfer of data to foreign countries and the possible need for more co-operation, all that is a matter for discussion with the Member States, and we are holding, as I said, a meeting on 22 November with experts from Member States to discuss those issues.

Q115 ***Lord Avebury:*** We have been, to some extent, bounced into making arrangements with a particular third country, the United States, and this may well happen again in the future, do you not think? To what extent have you been thinking about what the mechanisms should be for securing agreement amongst Member States if new demands are made by the US Homeland Security Authorities for data which is not at present legally transferable?
Mr Faull: We would hope that relations with, say, the United States would be the subject of discussion among our Member States before decisions were taken, and that decisions on transmission of data would be taken collectively, however controversial—as has happened with passenger name records, to which I thought you might be referring.
Lord Avebury: That is correct.

Q116 ***Chairman:*** Our favourite!
Mr Faull: Your favourite.
Mr Nunes de Almeida: Legally, that is data which has been collected by commercial companies which the American authorities then ask to have access to, whereas here we are talking about the sharing of information between—

Q117 ***Lord Avebury:*** Law enforcement authorities.
Mr Nunes de Almeida:—law enforcement authorities. There is where you have the gap presently: each Member State can do vis-à-vis the United States or any other third country what it wishes. That is the present legal situation.

Q118 ***Lord Avebury:*** Do you think there is a case for co-ordinating Member States positions regarding the exchange of personal data with certain States, or are you saying that is already covered by the meeting which you have just described?
Mr Faull: I think there could well be a case. It should be discussed on 23 November. I cannot imagine there will be immediate agreement among Member States on that, but it is clearly an area which we believe deserves careful consideration.
Lord Avebury: Thank you.

Q119 ***Viscount Ullswater:*** Does the fact that there are three pillars interfere with the co-ordination of data protection? We have data protection already fixed for the First Pillar and now it looks as if it is being developed for the Third Pillar. There must also be data protection on the Second Pillar as well, is there not? Are there different people looking at data protection on all those three fronts, or do they co-ordinate to try pull it altogether.
Mr Faull: Yes and yes. There are different people looking at this and we do try to co-ordinate. Our position is a very clear one: we look forward to the dismantling of the pillars. The Constitutional Treaty, now signed, will, when it comes into effect, bring that about. The pillars are a complication: we work with them, we work round them, we do not bang our heads against them, but we devote an inordinate, quite unnecessary amount of time to devising legal solutions to issues which straddle pillars. We have cross-pillar groups and all sorts of things. Of course, we understand their creation in the first place. We hope—and that only comes back to what I said initially—that over the years we have shown in our stewardship of the First Pillar aspects of Justice and Home Affairs, for which the Commission of course has a much more central role, that we have acted responsibly and sensibly and that gradually the First Pillar system or the Community method system could be extended to the full range of Justice and Home Affairs matters. At the moment, you are absolutely right: the data protection system in the First Pillar works well: the rules are clear. In the Third Pillar it all remains to be done, and that is what we are now doing. Where you have issues—as I am afraid frequently occurs—which concern both pillars, you end up with extremely complicated legislation, far from transparent and easy to understand, as we all want our legislation to be. I do not know much about Second Pillar data protection, I must say—we are not responsible here for those aspects—but my colleagues who deal with data protection are in contact with those who are, and we do try, where possible, to have similar answers to the questions which, after all, are much the same in all three pillars.
Chairman: Thank you very much. Could we move on now to areas of EU intelligence policy and a question about the Counter-terrorism Co-ordinator?

Q120 ***Earl of Listowel:*** Mr Faull, I would like also at this point to insert a question on training. Thank you for the helpful information in your presentation of evidence. I think we might all agree that training is often overlooked, and I would appreciate hearing from you as to what you think the role of the European Union will be in terms of ensuring that training is not overlooked. You have mentioned already the many languages within the European Union and we have talked about managing sensitive information. Perhaps you might also care to say something about CEPOL and investment in CEPOL. I understand that organisation has taken some time to get off the ground and now has a staff of only eight to ten people. Perhaps you may wish to comment on that.
Mr Faull: On training: of course, it is of the utmost importance, as we develop common rules and procedures and arrangements for co-operation and interoperability between our national bodies and systems, that the people concerned share some common training, some common understanding of the concepts which they are called upon to apply. We, as I said, try to make our rules and systems as simple and user-friendly as possible, but we all know that the legislative process usually conspires against that achievement and we end up with rather complicated rules and procedures, not made any easier by their existence in 20 languages. We were talking earlier about the "principle of availability": perhaps that is absolutely clear in Dutch—who knows—but in English we have to talk about it too! And so on. It is very important that we get the people concerned together and that they follow at least some sort of common curriculum in their training—and I do not mean initial training as much as ongoing training in their jobs. There are a number of ways of doing that. There are, of course, common concepts which can be introduced into the national training systems which every Member State will have organised in its own way, and we can provide information and materials, and we can encourage—and we sometimes have funding which can be used for this purpose—people from one Member State to go to another. There were, in the run-up to the enlargement of the European Union very extensive twinning systems in operation between the old Member States and the now new ones, and they have created networks of contacts

which should be maintained. We have a European police college, CEPOL, which is in the United Kingdom—we can say that now because its seat has been formally established in the United Kingdom—and we are now in the process of making it a proper European body by giving it a European legislative basis. So there is legislation now working its way through the system. Joaquim will have to remind me where it is.

Mr Nunes de Almeida: A proposal for a Council decision has been tabled, and it is now being discussed in the appropriate Council working group—actually today.

Mr Faull: Today.

Mr Nunes de Almeida: The European Council has decided the seat of CEPOL, Bramshill UK, and decided that it should have a legal personality. Now we have come forward with the decision explaining, in our view, what CEPOL should be. In our view, it should not replace the educational or police training by the Member States but its value-added would be to instil in the European police forces the European dimension that is probably missing or the possibilities for international or European co-operation. CEPOL would be like a technical body that would create a common education curriculum and common educational tools that could then be spread to other EU Member States, more than doing courses themselves. Because of the scarce resources it is probably more economic that they dedicate themselves to doing a common curriculum and educational tools that can then be disseminated to other EU Member States. Sometimes the education that matters for police co-operation is done by extremely easy issues or apparently trivial issues like languages. We were talking before about the principle of rights of equivalent access—yes, fine, but if you have a right of equivalent access to a Greek database, well . . .

Mr Faull: Good luck with the alphabet!

Mr Nunes de Almeida: Good luck, yes.

Mr Faull: It is a very small body, you are absolutely right, and it will remain a pretty small body for a very long time, probably for ever. It should be used, I think, as a lever for better training by the national police training colleges—which exist everywhere, of course—within each Member State. But we would have to see what the Council does with our proposal and how the thing develops a life of its own. In our conception, CEPOL will, as Joaquim said, devise training materials and suggestions to feed into the national training systems and will no doubt serve as a convenient forum for conferences and dedicated training sessions for police offices and others at various levels, but it should essentially organise better the network of national police training colleges which already exist.

Q121 ***Earl of Listowel:*** To return to the hymn sheet, the Commission Communication refers to exchange of information, but in your evidence you say there is a need for a common European Union criminal intelligence policy. How would you define information and intelligence? To what extent can an EU level intelligence policy be developed that does not cut across the priorities of individual Member States?

Mr Faull: The Commission Communication refers to exchange of information and also to the need to provide law enforcement authorities with the relevant and needed information. It then goes on to consider the core elements of an intelligence-led law enforcement capability to be set up. The terms "information" and "intelligence": In our understanding, information encompasses various types of data in the public domain collected for business purposes: statistics; information on emerging threats; and so on. To cover all these sources of information, these types of data, the notion of equivalent access, which we discussed earlier, has been developed to ensure that the information can be made available for law enforcement purposes. Intelligence, on the other hand, we understand as being the first interpretation of information, and intelligence for law enforcement purposes we understand under the notion of criminal intelligence. We do not in any way intend the development of a European criminal intelligence idea to replace or to jeopardise systems or developments at national level. We want to provide added value to initiatives taken at national level. We currently face a situation where the law enforcement authorities of the Member States do not always have the criminal intelligence they need to guide their work when a threat is perceived to concern the Union as a whole or a large part of it. Our aim is to develop a methodology to allow the use of standardised analytical tools based on relevant law enforcement information available within the Union. We are very much at the beginning of our work in this area and look forward to extensive discussion with the Member States at all levels for the preparation of a report to the Council which we intend to make by the end of next year.

Q122 ***Earl of Listowel:*** I suppose an advantage to an individual State is that they have here an opportunity to obtain the support of all of the EU for their major concern if they are successful in the negotiation.

Mr Faull: Indeed. Terrorism is an international business and the response to it requires international co-operation. Since in the European Union we have the mechanisms of the Union available to develop and make meaningful that co-operation, we think they should be used. We also have in the Union, of course, remarkable ease of movement of people, of goods, of money across our territory. Globalisation has made that possible generally and of course the

developments of the Union in the last 20-odd years have made that even more tangible for European. That means that, while the 99 per cent of *bona fide* beneficiaries of the system can enjoy it, terrorists can also take advantage of our openness. We therefore need to develop together a response fulfilling the need to combat terrorism within the European Union.

Q123 ***Earl of Listowel:*** In your evidence you made the distinction between strategic and operational intelligence. Could you explain that a little further, please?
Mr Faull: Yes. When intelligence is produced by using information, it can be used to provide a clearer view on what threats need to be addressed as part of an overall strategy, both at a tactical immediate level and as part of a wider strategic view. Once this has been done, criminal intelligence can be used to provide guidance on how to deal with specific threats and crimes and what priority should be attached in the law enforcement system to particular items. It is essentially a matter of level. There is an overall strategy—a crime prevention strategy, a law enforcement strategy—in each Member State, of course, within which priorities have to be allocated and then there are operational needs dealing with a specific case, a specific type of crime.

Q124 ***Chairman:*** Could I ask whether you believe there is a difference between national security intelligence (that is, terrorism) and criminal intelligence. Do different countries have different views on what that might be?
Mr Faull: No, I do not think they do, if they conceptualise it in quite that way, because the borderline between terrorism and other types of organised crime is an increasingly blurred one, and I think everybody understands that today. That does not mean, however, that Member States do not have perhaps excessively compartmentalised distinctions of this sort in their structures and in the way their intelligence systems operate, but, more and more, they find and we find that criminal intelligence reads across into counter-terrorist intelligence, and, indeed, vice-versa, and it does not make much sense to deal with the issues separately. That said, of course, there are types of crime which seem to bear no—and we can always be surprised—immediate relevance for the fight against terrorism, where the normal criminal justice system, the criminal-intelligence-gathering systems of each of the Member States, will carry on untouched by developments in the counter-terrorism field.

Q125 ***Chairman:*** Do different countries have different views on that or would they share your analysis of that?
Mr Faull: I think they are increasingly sharing that analysis. But some Member States, perhaps fortunate ones, have never experienced terrorism to any significant extent on their territory. We discovered after 11 September 2001 that some Member States of that time, the 15, did not have a definition of terrorism in their statute books: they had never needed one. Lucky them. Suffice to say, we have introduced a common definition. There is today, I think, a growing understanding that no EU country is safe from terrorism and certainly that no country can consider itself unlikely to be used as a base for some of the preparations of terrorist activity, if only because, in our wide internal market, money, people and goods can be moved around so easily. Secondly, the growth in international terrorism is there for everybody to see and everybody feels threatened by it and part of the collective effort to deal with it.
Chairman: I would certainly share your view there. I was recently in another Member State, an old Member State, and I was very, very surprised to hear that they do not really regard terrorism as being terribly important to them. This is very concerning for all of us. It is the level at which each Member State feels they should participate in all these activities to try to undermine terrorism.

Q126 ***Lord Avebury:*** Earlier on you said in answer to Lord Listowel that intelligence provides a clearer view of threats that need to be addressed. We have been skating around a particular threat, the growth of Salafist terrorism, which is worldwide phenomenon of which we have seen examples in Europe more than in other parts of the world following 9/11, as you know. What is the capacity of the European Union to address the strategic origins of this movement? In other words, do you have people who are experts in the Salafist and Deobandi ideologies of Islam in which the terrorists are embedded? Do you promulgate that information to the Member States, who, as the Chairman has said, may have a very limited appreciation of the nature of this threat?
Mr Faull: Yes, we do have foreign affairs specialists, both here and across the road in the Council of Ministers under Javier Solana, and they work closely with the specialists in the Member States, which of course have a much broader range of foreign policy expertise, in ministries in their capitals, in their network of embassies abroad and in their intelligence services. We are keen, of course, to make sure that that information is shared by the big Member States, with traditions and resources and language skills and extensive diplomatic networks, with the smaller Member States, which, do not have that range of information available to them but may need it. The difference between the range of skills and experience and information of, say, the British Foreign Office on

the one hand and the Foreign Affairs Ministry of a small new Member State on the other, is obviously quite extraordinary, and we should not allow—and this is, I think, a danger for all of us—a mistake to be made or a piece of information to be ignored because the expertise in one place is not known about and put to good use in another. Again, that is easy to say, hard to bring about, because some of the information which the well-resourced Member States will have will be information which can be provided only with difficulty because of the danger of revealing sources or the method used to obtain it. We have, over in the Council, the Situation Centre and we have all sorts of mechanisms where the foreign affairs specialists of our Member States come together to discuss specific topics, issues in particular parts of the world—terrorism, of course, and all its various ramifications are often high up on the agenda. I cannot be sure—it is not our immediate responsibility in this department—how effective it is, but our hope is that the information exchanged formally and, perhaps more importantly, informally between the foreign affairs establishments of our Member States covers the sorts of issues to which you have referred.

Q127 ***Lord Wright of Richmond:*** Could I ask a supplementary speaking as a former British Ambassador to Saudi Arabia? Are you conscious of any diplomatic reports by combined representatives of the EU in the capitals abroad? I am just wondering whether, for instance, the ambassadors in Riyadh have ever put forward assessments of the terrorist threat from Saudi Arabia. This is probably Javier Solana's portfolio.
Mr Faull: It is. If they did, they would not come here, they would go to our External Relations Directorate-General or to Mr Solana's people. But what should happen in a well-run diplomatic outpost of importance such as Riyadh would be regular meetings between the head of our delegation there and the Member States' ambassadors, plus of course between their colleagues at lower levels. That should be the place where co-ordination takes place and is reported back here, as well as to the national capitals. I do not know how good it is.
Lord Wright of Richmond: Thank you.

Q128 ***Earl of Listowel:*** You say in your evidence that an EU policy operational intelligence "has to take full account of the specific law enforcement culture of each Member State." I think we have just been talking about one aspect of that. What practical steps can be taken to achieve this?
Mr Faull: As we have said, there are different approaches today among the Member States to the collection, use and exchange of information—information which is the raw material for the production of useful intelligence—and other differences, as we have seen, arise when we look at the ways in which law enforcement authorities can obtain such information within their territory or across the Union. These differences no doubt arise from and give rise to what we can call different law enforcement cultures in the Member States: the importance of data protection; the allocation of priorities within the criminal justice system—all these things will vary from one country to another. The Chairman said earlier that some countries have not yet put terrorism at the top of their law enforcement priority list because they have been lucky enough not to have to deal with it and perhaps are not farseeing enough to consider the threat for themselves. We do not want to change national cultures; we want to understand them better. Without disturbing them unnecessarily, we want to promote ideas from one where we think—and others can be brought to think as well—things are done particularly well; we want to promote best practices, to offer to the others—with of course full allowance for the massive differences in resources available between a large country and a small one—so that a common understanding can be developed of what is necessary in these areas.

Q129 ***Earl of Listowel:*** Could we move on to the Counter-terrorism Co-ordinator? You seem to envisage the role of the co-ordinator as one of overseeing the implementation of EU counter-terrorism legislation and producing papers for discussion in the Council. Is there a case for giving him a role in co-ordinating operational action of the various competent bodies in the EU? Could he also represent the EU in international fora, given the need which you have emphasised for the Union to speak "with one voice" in these matters?
Mr Faull: Certainly we believe that the role of the Counter-terrorism Co-ordinator should encompass the tasks you refer to which we have put forward. They are important. We find, frustratingly, that the level of compliance by Member States with commitments they have entered into is disappointing, and there is clearly a need for better enforcement—not in the legal sense, because, unfortunately, in the Third Pillar there are very few legal enforcement mechanisms available to us, but there we need to bring about better compliance by Member States with the decisions that they have taken. Mr de Vries, the Counter-terrorism Co-ordinator, clearly has a very important role to play, particularly in the Third Pillar, in cajoling Member States into doing the things they have signed up to. We believe also that the Co-ordinator can play an important role in operating within the Council system for the benefit of the Situation Centre, where an important job is to be done in the area of counter-terrorism related intelligence. I do not believe that the Co-ordinator has the resources, the mandate or the

institutional position to co-ordinate operational action of the various bodies in the European Union. The Council Secretariat is not an institution in its own right, and we do not believe—and I have no reason to believe the Council Secretariat would believe this either—that it has the budget or the capability of co-ordinating others' operational activities. An analogy with the Second Pillar might be of interest here. The actions established under the Second Pillar's common foreign and security policy are implemented by the Commission. Operational co-ordination can relate to two distinct categories of activities: those conducted by the Commission and those conducted by other Union bodies, such as agencies. The Commission's operational activities relate to tasks entrusted to it by treaties or by legislation; for example, in the area of civil protection. The Commission cannot give up such responsibilities or submit them to co-ordination systems not provided for by the treaties. We have, it seems to us, the expertise and the resources to carry out the operational task entrusted to us, and to draw on the networks created with counterparts in the Member States in order to do that. As regards the operational activities of other European Union bodies in the field of intelligence and law enforcement, we believe it is very important to continue the work to consolidate, strengthen and develop Europol, and we do not see how the Counter-terrorism Co-ordinator could assume a co-ordination role over Europol. Finally, as regards external representation of the Union, this is carried out by the Presidency and the High Representative, Mr Solana, on the one hand and by the Commission on the other. Within the Presidency/High Representative delegation to international fora, an important role can, of course, be played by the Counter-terrorism Co-ordinator. That indeed happens, and it all works smoothly. The Commission, of course, plays its own role, separately but in harmony with the other institutions.

Q130 ***Lord Wright of Richmond:*** We are seeing the Counter-terrorism Co-ordinator this afternoon, so this is a question that would probably more properly be put to him, but how clear is his job description? Is it clearly understood? Is it actually written down what his job is?

Mr Faull: It is certainly written down in the conclusions of the European Council creating the function, inevitably in rather general terms. I am not aware—but certainly you can ask him this—whether he has developed a more detailed job description within the Council system. I have to say that our relations with him are extremely good, co-operative and friendly. We see his role as very much complementary to our own and I hope he sees it in the same way.

Q131 ***Earl of Listowel:*** In their response to the five-year programme for an area of freedom, security and justice, the European Parliament Civil Liberties Committee criticised the arrangements for the Counter-terrorism Co-ordinator in terms of accountability and the weakening of the Community character of the executive. They called for greater parliamentary scrutiny of the activities of the Co-ordinator and a review of his links with the Commission. Do you think there is any force in this criticism? How does the Commission relate to the Co-ordinator? Both the Commission and the Co-ordinator presented reports to last week's JHA Council. Is there an element of duplication in their work? In what direction should the Commission's relationship with the co-ordinator be reviewed? You may have covered some of this in what you have already said.

Mr Faull: Yes. I do not see a problem of accountability relating to the exercise of non-executive functions by the Counter-terrorism Co-ordinator. His work in co-ordinating the work of the various Council bodies is, I think, a matter for the Council's internal working, and the Council, of course, through the Presidency, is regularly in contact with the Parliament in giving account of the work it is doing. Co-operation between the Commission and the Co-ordinator, as I said, is extremely good. There are frequent contacts, more often these days—and I think, this is very much to our mutual benefit—informal than formal. I am in regular personal contact with Mr de Vries and I do not think there is any duplication of our work. In fact, this has worked in practice rather well: where the Council or the European Council invites the Commission and the High Representative to work on a specific issue, we have done that, initially separately, but in fact in informal contact with each other, and then, often at the COREPER level of permanent representatives, of ambassadors, work has been merged together, with our full agreement, into one document for the Council of Ministers or for the European Council. We are complementary. Where we are working on similar issues but from different vantage points, our work can and does converge and become one common document for ministers.

Q132 ***Lord Avebury:*** Why was there not a common document in the recent presentations to the Council? Why were there two separate documents?

Mr Faull: Because this is work being prepared for the European Council in December, and you will find that by then the documents will be agreed by the Council Secretariat (in this case) and the Commission, and if documents can be merged they will. It is still a preparatory step.

Chairman: Thank you very much indeed. We will now move into our final tranche of questioning around institutional structures. Could I ask Lord Ullswater if he would ask these questions.

Q133 ***Viscount Ullswater:*** I would like to quote two things from your written evidence. "Several Council or other EU structures are currently dealing with aspects of the fight against terrorism with little overall co-ordination at EU level."
Mr Faull: Did I say that?

Q134 ***Viscount Ullswater:*** It seems to have come under your signature.
Mr Faull: Oh, dear. All right.

Q135 ***Viscount Ullswater:*** Also, you made the comment that: "Mr de Vries could contribute to further improving the Council working structures on terrorism." Yet I understand that the European Council on 25 March in its Declaration called for new institutional structures to be put in place. Has anything happened? What changes in fact are being looked at? When I read your evidence and then was interested in seeing what was currently happening, it looked as if the two things were slightly out of step.
Mr Faull: Yes. Well, perhaps I was a little harsh in my written evidence because I do not want in any way to demean the very considerable efforts that Mr de Vries is making and that we are making within the Commission. The starting point for all this is that counter-terrorism spreads across a wide and probably increasing number of policy fields: banking for money laundering; transport issues for transport security; customs; border management; environment; public health—all of these areas—and, of course, what I am saying is matched very much by co-ordination needs and efforts taking place at national levels. Ministries and departments and Commission Directorates-General and Council configurations are faced with a growing need for co-ordination to deal with subjects with which some of them have not traditionally been involved very much. It is therefore necessary to enhance co-ordination as much as possible and the question arises whether we have the right bodies and structures for dealing with this. We all know what the Americans have done, following 9/11, in the creation of the Department of Homeland Security: a massive bureaucratic upheaval, the creation of a new department. That is not what anybody is suggesting on this side of the Atlantic, but we do need to make sure that all the various bodies and organisations with a stake in counter-terrorism are working with each other, are—to use the expression we used earlier—properly interoperable, interoperating, because the risk of missing a link between two bodies, between two items of information is so great that it is clearly incumbent on those responsible for public policy that that risk be minimised or eliminated altogether. Now, as is the case everywhere, the various structures we have inherited from the past were not designed exclusively in any way to cope with counter-terrorism. Customs authorities suddenly have to cope with container security, port security, airport security and so on, just as our colleagues in public health are having to deal with the threat of bio-terrorism and so on. The Council on the other side of the road also has a different set up, based on the provenance of the ministers who come to meetings, so you will find the ministers of finance talking about the money laundering aspects of terrorism; you will find the foreign ministers talking about the foreign relations aspects of all of this; you will find the environment Directorate-General here responsible for civil protection and so on. Our role here in this department is to co-ordinate all the Commission's work in this area and I think we do it pretty well, and Mr de Vries's job over in the Council is to bring together the various Council formations and the officials involved in the preparation of their work, so that there is a consistent policy and legislative response to terrorism. It is also the case that, again, in different times—in more innocent times—we had various bodies created at European level: we have CEPOL, which we talked about earlier, the police training college; Europol; Eurojust; the Police Chiefs Task Force. We have these various bodies and we have to be absolutely sure that they are operating to full potential and that they are operating with each other in the best possible way. Have we achieved that? No. We can always do better. I did not mean to be overly critical in the rather stark statement I made in the written evidence, and it is criticism I would make of myself as much as of anybody else: we can always do better to join up the various bodies and structures that we have created, and, where they do not seem any more to serve a useful purpose in their current structure, we should be prepared to change them. We have the complicated legal situation of the three pillars. We have the Constitutional Treaty coming, we hope—now signed but still to be ratified—and we are aware that that will not be an easy process in some Member States. Therefore, we have a period of legal uncertainty in which to operate, but we should do our very best with the legal framework we have. The line taken by the Justice and Home Affairs Council and then the European Council in the aftermath of the tragic events in Madrid on 11 March of this year is that we do not need new bodies or new initiatives in the European Union so much as getting the full potential out of what we have already. That means Member States doing what they have promised to do and getting Europol and Eurojust working properly together, rather than assigning new initiatives which may

attract headlines in the days following a terrorist attack but which actually may not add very much to the real work being done in the first place.

Q136 ***Viscount Ullswater:*** I am not sure whether you answered the question whether there are some new institutional structures being called for. I gathered from your reply that you were really suggesting that what was there at the moment should work better, but, if my information is correct, the European Council has actually called for new institutional structures. Is there something that we should know about?
Mr Faull: Of course! You should know about everything! On 25 March the European Council created the function of the Counter-terrorism Co-ordinator and endorsed and called for the implementation of an updated plan of action on the fight against terrorism. The Europol Counter-Terrorism Task Force was reactivated and it is considering how best to integrate the Chiefs of Police Task Force into our institutional system. The Europol Information System is being set up and joint investigation teams have been created between Member States—Spain and France have been very active in this area—and we will establish a European border agency to improve the management of our common external border in 2005. A key issue, it seems to us—and we are interested in the UK's intelligence-led police model on European criminal intelligence—is how best to bring the Chiefs of Police Task Force into our institutional structure as a strategic and operational forum on crime within the European Union. We must find a way to bring that task force into our system and link it in with work being done by Europol.

Q137 ***Viscount Ullswater:*** Thank you. I think you have answered how best to co-ordinate the activities of Europol, SitCen and the Police Chiefs Task Force. You say, again in your evidence, that they are outside Council structures. Is that a dimension which makes them harder to deal with or is it a funding operation which means there is a difference between the two?
Mr Faull: No, it is not, so far as I am aware, a question of money at all. This task force brings together the heads of our police forces. It is obviously an extremely high level group of people, and there is a certain sense of frustration on their part and on ours that the work that they do is not fed into the policy and legislative systems of the Council of Ministers. So the key is how to bring the Chiefs of Police Task Force into that system without disturbing excessively the normal hierarchy of civil-servants-up-to-minister structures of the Council of Ministers. But it is clearly important, it seems to us, that the Police Chiefs Task Force be more than a purely consultative body, where we just put a few problems to them, they give us the benefit of their views, and they do not know precisely what use is made of them later. It seems to us that they should be plugged in, not to Commission level but to Council level, so that when the Council is considering policy or law it has the benefit of the operational input from the people who are going to have to enforce it.
Mr Nunes de Almeida: It is a question of preparation and follow up, in the sense that, if they are situated outside the Community and the Union's decision-making process, their meetings are not adequately prepared by a staff which is dedicated to their operation and so there is no proper preparation and follow up. They meet, but then it is as if there would be a missing element for their ideas to be brought about into the operational arena.

Q138 ***Chairman:*** There will always be concern expressed by police chiefs that there could be operational interference and it is difficult to get the balance right between getting the intelligence out from what they have been discussing and nobody interfering with how they want to deal with an operational incident. It is a very tricky area to get right.
Mr Faull: Yes. We are well aware of that. We are guided to a considerable extent by their own frustration at their current position. They acknowledge and welcome the need to work together. They believe that they have important and interesting things to say to policy makers and law makers and we have not quite found the right channel to plug them into that system. I understand your point about what happens downstream, when it comes to operational implementation, where, of course, the balance between the police force on the spot and the politicians and administrators who make the rules is a very delicate one.

Q139 ***Chairman:*** And there all sorts of issues around transparency and accountability, and where they will be put in.
Mr Faull: Yes.

Q140 ***Chairman:*** The question of how we could operate more closely together must go alongside transparency and accountability.
Mr Faull: Yes. If I may make a final point on this, the Constitution, when it comes, will create the Internal Security Committee—we say "COSI" in French, which makes it sound rather nice—and the Dutch have been giving thought to how, without in any way pre-empting the entry into force of the Constitutional Treaty, the preparation for the creation of that committee could be a useful way of concentrating minds on the need to simplify and rationalise the systems we have already in the existing legal framework today. We will have to see how that

comes out of the discussions on the Hague Programme.

Q141 ***Viscount Ullswater:*** That really strayed into the next question, which is about the proliferation of groups within the European Union concerned with counter-terrorism. There is a terrorism working group for Pillar three, there is a terrorism working group for Pillar two. I think you were just about to say that there is scope for streamlining this or for bringing it closer together, so that people do not seem to be working in isolated pockets.

Mr Faull: Yes, obviously necessary. I do not want to suggest that the current situation is a desperate one. There is already an enormous amount of co-ordination work done by my Department within the Commission. We have an internal working group which I chair with a colleague in the External Relations Directorate-General, which brings together everybody dealing with the internal and the external aspects of terrorism within the Commission, and immediately below our level there is an internal group, chaired by my director responsible for counter-terrorism, and an external group, chaired by the external relations people at director level as well. Within the Council we have talked about the very important role of Mr de Vries and then everything comes up through the Council system to the ambassadors, to the permanent representatives in COREPER, and that is where an overall governmental view should be established in each capital reflected by the ambassador in COREPER, and the various strands of counter-terrorism policy, whether they originate in banking or in the environment or here or in external relations, should be brought together in one coherent, composite view. From those 25 governmental views should come a collective European view. That is the way the system works and nearly all the time it works extremely well. We have, despite the risk of proliferation, already put co-ordination systems in place which prove effective; nevertheless, of course we could do more. We have the prospect in the Constitution of the COSI coming on stream, and the possibility to improve matters under the existing legal framework, by taking such steps as are necessary to bring the Police Chiefs Task Force more operationally into the Council system as well.

Q142 ***Viscount Ullswater:*** You seem to be rather critical of developments within the G5 framework. Do you have causes for concern there? Is it perhaps not unrealistic to expect that all discussions take place at the 25 member level?

Mr Faull: To be effective, measures to improve law enforcement co-operation in the fight against serious crime and terrorism need the active participation of all Member States. The Union framework, it seems to us, is the appropriate one for discussion of these things. It provides legal back-up, where the law is necessary to give effect to policy, and the security of all of the European Union's residents and their right to live in an area of freedom, security and justice is one which should apply to all of them in whatever Member State they may live. So it is very important that the Union's systems be used to develop policy and to make rules where that is appropriate. Of course there are many operational matters which groups of Member States, for various reasons, wish to discuss amongst themselves in smaller groups. The Nordic countries have a group; the Benelux countries work together; the so-called G5 Member States come together; among the Mediterranean Member States there are obvious issues they wish to talk about amongst themselves which have less relevance to the Finns and the Swedes; there is a group called the Salzburg group, which brings together Austria and many of its neighbours. The Commission has absolutely no objection to Member States coming together in various ways to discuss matters of common interest. But, where we are talking about policy developments, it is our view that the Union's systems and mechanisms should be used and only when it is shown that it is not possible to reach an agreement among the Member States, among the 25, using whatever system of adoption of decisions is provided for (qualified majority voting or unanimity), then we have the system of enhanced co-operation which Member States are entitled to use. To repeat, because I think this is important: there is absolutely no objection to Member States meeting at ministerial or other levels to discuss issues of common interest in whatever groupings they find most appropriate, but, where it comes to addressing issues which really are of common interest to the whole of the Union, we would want to see the Union's institutions and mechanisms used. They provide considerable added value by being part of a fully fledged legal system and bringing in the accountability mechanisms with the European Parliament. Where it is not possible to make progress among all 25, or using qualified majority where that is available, then enhanced co-operation exists as an alternative mechanism.

Viscount Ullswater: I think that was rather a reassuring answer, because obviously you recognise that it would be only fair to think that smaller groupings, with problems which concern themselves rather than the whole 25, could meet and talk about them.

Q143 ***Chairman:*** Could I wrap up today's session with a question about the new proposals which you presented last week to the JHA Council. I wonder if you would be good enough to outline the main elements of that.

Mr Faull: With pleasure. The first communication called *Prevention Preparedness and Response to Terrorist Attacks* sets, in effect, the other three against the general framework of what the Commission is doing to implement the action plan on the fight against terrorism. Essentially, it espouses the notion that the fight against terrorism must be not only integrated, bringing together all policy strands, but also inclusive, bringing together all of the so-called economic and political actors. It proposes a novel way of involving citizens, civil society and parliaments in a process of reflection on how to strike a balance between the various policies involved in achieving the common objective of defeating terrorism. We therefore want to foster a civic and democratic debate on securing freedom. We suggest that the Union should honour the victims of the dreadful attack in Madrid on 11 March by producing, before 11 March next year, a memorial report, which would be addressed formally to the European Union and to national parliaments, describing what has been done in the fight against terrorism since 11 March 2004 and what are the challenges ahead of us. It proposes a public/private security dialogue with industry and other economic actors, stresses the cross-cutting importance of security research and mentions the recent report by a group of wise persons advocating additional funding of €1 billion per year for security-related research from 2007 onwards. That is in the new financial perspective.

Mr Nunes de Almeida: Yes. It is an idea they had for the research framework programme.

Q144 ***Chairman:*** From 2007 onwards.

Mr Faull: Yes. That is for the next budgetary settlement. The communication on *Preparedness and Consequence Management in the Fight against Terrorism* gives an overview of activities already under way in the Commission and proposes additional measures to strengthen the existing civil protection instruments and consequence management arrangements. We need to ensure that relevant information is shared instantly with all Commission departments and national authorities concerned. Some emergency situations may be of such gravity and pose such a risk of degeneration into a major crisis that overall co-ordination across virtually all EU policy areas is necessary. Therefore, co-operation and co-ordination between the Rapid Alert systems created in the Commission need to be properly secure. Therefore, we propose the creation of a General Rapid Alert system, to be known as ARGOS, to link all specialised systems for emergency alerts requiring access at European level. The new system will respect the specific characteristics and expertise of individual specialised systems managed by the Commission already, which will continue to carry out their functions. However, since it is often unclear in the initial phase of an incident whether it is an accident or a terrorist attack and whether there are bio-terrorist or other causes and consequences likely, co-ordination of all the crisis centres and rapid reaction mechanisms is absolutely essential. We will create within the Commission a central crisis centre—one phone number, one e-mail address—which will bring together representatives of all relevant Commission services immediately during an emergency and co-ordinate the network of national crisis centres already in place in the Member States. A law enforcement network should be established to be managed by Europol and linked to ARGOS to serve the needs of the law enforcement community in an emergency. The communication *Critical Infrastructure Protection in the Fight against Terrorism* provides an overview of activities under way in the Commission on the protection of critical infrastructure, and proposes additional measures to strengthen those instruments, mainly by the establishment of a European Programme for Critical Infrastructure Protection (ECPIP) which would provide enhanced security for critical infrastructure as an ongoing annual system of reporting and review, enabling the Commission to put forward its views on how to ensure that critical infrastructure would continue to operate in the event of a crisis. An EU Critical Infrastructure Warning Information Network would be established to assist Member States, as well as owners and operators of critical infrastructure, to exchange information on shared threats and vulnerabilities and appropriate measures and strategies to limit risk in support of critical infrastructure protection. Where standards do not yet exist, the European Committee on Standardisation (CEN) and other relevant standardisation organisations should be asked to propose uniform security standards for the various branches and sectors concerned. Standards should also be advocated at the international level through International Standards Organisation (ISO) to establish a proper level playing field in that respect. The communication *The Prevention of and the Fight against Terrorist Financing* focuses on the need to improve information exchanges between relevant parties at national, European and international levels. We need to improve co-operation and systems for exchange of information between tax authorities, financial supervisory bodies, justice ministries and their counterparts elsewhere, the intelligence communities, law enforcement authorities and the authorities in charge of administrative freezing of assets. One of the more controversial ideas in this area is to give law enforcement authorities access to financial institutions' databases of account holders and their transactions. This would allow for the

linking of information, identifying flows of money and tracking sources. Of course, there are serious data protection issues to be considered there, but the issue was flagged up as an obviously important one. We need to improve the traceability of financial transactions. This means that Member States should ensure that their law enforcement services have sufficient resources to develop the necessary financial skills to enable them to trace money trails backwards to the people providing finance and forward to the terrorist cells using the money. There, of course, the differences between resources and skills in the Member States are still quite considerable. Therefore, training is, once again, of enormous importance, and the development of minimum standards for training and co-operation between Member States in training is extremely important.

Q145 ***Chairman:*** Thank you very much indeed. You can see that we have been scribbling madly getting all that down. It is very impressive.
Mr Faull: Since those communications came out after I submitted written evidence, I would be quite happy to give them to you in writing.

Q146 ***Chairman:*** That was going to be my next question. Thank you very much indeed. You have been enormously helpful. You have given us a huge amount of information. It is a very challenging time for the Commission to implement this very, very exciting programme. Mr Faull, thank you so much, you and your team. You have put an enormous amount of effort into answering all the questions that we have laid at your feet and we do appreciate that most sincerely. We know that when we come to ask for your time, your very valuable time, you have a lot of work to do before we come, so we are very grateful to you. Thank you once again.
Mr Faull: May I thank you all for coming. It was good of you to travel out to Brussels. We admire the work you do. We read your reports with great interest.

Q147 ***Chairman:*** We hoped you would say that!
Mr Faull: I can tell you that they have considerable influence across the European Union because you go to such trouble in producing work of high quality. Therefore, the work done by the House of Lords is much admired throughout Europe and it is certainly taken very seriously by the Commission.
Chairman: Thank you very much indeed. If we can be of help in any way in the areas of JHA, then we are only too happy to do so. Thank you again.

WEDNESDAY 3 NOVEMBER 2004

Present: Avebury, L; Harris of Richmond, B (Chairman); Listowel, E; Ullswater, V; Wright of Richmond, L

Examination of Witness

Witness: MR WILLIAM SHAPCOTT, Director, Joint Situation Centre, and Special Adviser to Javier Solana, Secretary General of the Council, examined.

Chairman: Could I thank you on behalf of the Sub-Committee for entertaining us and for being willing to answer our questions. You have had sight of our questions and there will be supplementary questions arising out of the evidence we have heard already today. I hope you will bear with us while we ask those. Before I start, perhaps I ought to register the fact that members have declared interests in this particular inquiry. For instance, my interest is that I was former Chair of the Police Authority and was a member of the National Crime Squad Service Authority and I am a JP on the Supplemental List.
Viscount Ullswater: I am a JP on the Supplemental List.
Lord Wright of Richmond: I suppose I have to declare an interest as the permanent under-secretary who received you into the Foreign Office! But, more seriously, as Chairman of the Joint Intelligence Committee 20 years ago.

Q148 ***Chairman:*** I wonder if it would be helpful if you made an opening statement before we launch into our questions.
Mr Shapcott: Could I just clarify the position vis-à-vis on and off the record.

Q149 ***Chairman:*** Whenever you want to say anything off the record, if you say, "I would like this to be off the record," the machine will be switched off, and only when you say "Now going back on the record" will it be switched on. There will be no other reference to what you say off the record anywhere in our report.
Mr Shapcott: But the record of evidence will in due course make its way into the report?

Q150 ***Chairman:*** Absolutely.
Mr Shapcott: Which will be fully published?

Q151 ***Chairman:*** Which will be fully published and go all over Europe.
Mr Shapcott: That is useful to know. You would like me to concentrate principally on the counter-terrorism field or more generally?

Q152 ***Chairman:*** On the counter-terrorism field mainly and on what JSC does.
Mr Shapcott: Unless you stop me, I propose to make about a 15-minute introductory statement. The Council Secretariat and the Council indeed changed radically with the entry into force of the Amsterdam Treaty in October 1999. At that point, two particular institutions were established, the post of Secretary General High Representative, filled since that date by Javier Solana, and the establishment of a Policy Planning and Early Warning Unit. These two practical steps were intended to be valuable aids towards the development or further development of a Common Foreign Security Policy. CFSP had been instituted at the time of the Maastricht Treaty and was evolving: it had started in a rather declaratory mode but clearly the Member States were by the late nineties keen to see it move in a more substantial direction and these two elements were intended to add to that. The Policy Planning and Early Warning Unit was staffed by a diplomat per Member State (and I initially came into Brussels as one of that team) but it was intended as a nucleus of support for Solana, of policy-oriented officials with links to their national diplomatic services who could supply him with information, with advice—both inputs from those countries but also independent advice as they developed their own contacts working on his behalf. As these two entities arrived in Brussels, it became pretty obvious to them that if he, Solana, was to start making solid policy proposals to the Member States he needed to do so on the basis of good information. There was an element in one of the declarations to the Treaty in which the Member States undertook to provide confidential information to this apparatus to assist in policy development. I am not sure that those who made the declaration understood quite what they meant by "confidential" but they meant "special": information of a special character, and when the team arrived this was interpreted to mean some reporting from their diplomatic networks across the world. So, in the early days, several of those Member States were supporting Solana by showing him or briefing him on what the main diplomatic flow from their networks was saying about developments in countries of interest around

the world. This was a great help to him. It was no surprise that the British input was strong, and he has appreciated the British input over time. But this was very much focused on the diplomatic channel. This situation prevailed for a couple of years. Solana was clear right at the beginning that this information exchange would probably need to go further than diplomatic information and to include intelligence information, that he also appreciated that the sharing of intelligence in a multi-national environment was something which you probably had to let come to you rather than go out and promote and pull. Indeed, he was shown a paper fairly soon after he arrived that suggested setting up some sort of mechanism, and he said, "No, we really need to wait for the Member States to come forward with ideas in this area." So the situation continued for a couple of years. I think—but you are outside observers: you would have a better view—the Union's Common Foreign Security Policy has improved in that period, clearly not just because of these information exchanges but because the Member States wanted it to improve, they wanted it to be more effective, and they have supported Solana and supported the new structures. By 2001, around the time of 9/11, a number of Member States approached Solana to say, "We would like to go one step further. We would like to start sharing more sensitive information. We would like to see an attempt made to undertake common assessments of particularly critical issues in terms of the Union's foreign policy." Several Member States made this approach. Solana thought that the time had come and he decided to give the Situation Centre, which had existed as a sort of empty shell until then, a particular intelligence assessment function, and we set about establishing which Member States would like to participate and were prepared to send information. Since the very end of 2001/beginning of 2002, a substantial number of Member States have supported this project, through sharing sensitive information, generally assessed intelligence, and this has been used to develop common assessments on issues of interest to the European Union foreign policy. Clearly you cannot do foreign policy without considering the issue of terrorism, so, from the early days, this entity evaluated a number of situations where terrorism was a factor, looking at risks to European interests abroad, looking at risks to the stability of friendly governments threatened by terrorism abroad, but very much with a Second Pillar focus, supported by the external services of the Member States. In the period in which we were doing this, and I suppose in 2003 particularly, it became fairly evident, as it has become evident in a number of Member States, that to look at terrorism in internal and external terms or Second Pillar and Third Pillar terms is a little bit artificial. Clearly the terrorist networks do not make this distinction, why should we handicap ourselves by doing the same thing? Contemporaneous with this, a group called the Counter-terrorism Group began to develop a capability of its own. After 9/11, the justice ministers called for the security services to meet as a group, and they called this group the Counter-terrorism Group (CTG). It was really the Berne Club under another name, because in fact Norway and Switzerland continued to be parties, but it dealt only with terrorism, whereas the Berne Club deals with a wider range of internal security issues, including counter-espionage. We became conscious of the work of this group during the course of 2002–03 and their analytical work is very interesting, as you would expect, but it was divorced from the Union. There was no institutional connection to the Union, and material was shared on a personal basis with a few figures in the Union but it was not discussed in the Council, it was not discussed in the Committee of Permanent Representatives, it was not discussed in any of the working bodies. Putting these two things together, the idea that we should stop looking at terrorism purely as an external issue and look at it in a more comprehensive fashion, and the realisation that a good deal of good analytical work was being done but not being well used, we hit on the idea of making a connection between these two activities, so connecting the co-operation between external services in the SitCen with the co-operation between internal services and the Counter-Terrorism Group. This was an idea which we kicked around a bit with Solana. A number of services in the Counter-Terrorism Group thought we should move in this direction, but this is a reasonably sensitive area. Our assumption was that this would move fairly slowly. I expected it would probably take about two years to engineer the necessary co-operation. Also in 2003, Solana had been asked by the Member States to produce a European security strategy. This was agreed by the European Council at the end of 2003 and it included the notion that terrorism was one of the key threats to European interests. At the European Council at the end of 2003, Solana was asked to come forward with ideas for implementing the strategy: to take it from a conceptual document towards more policy-related proposals. He started working on this and one of the *volets* in this follow-up work was a paper on terrorism which he put to the Committee of Permanent Representatives in February of 2004. This was, like many things in the Union, supposed to be an internal paper, but, because it was interesting, in that he was rather critical of the existing institutional arrangements, it fairly quickly moved into the public domain. But a couple of the key points were a sense that we should get away from the Second Pillar/Third Pillar division; that we should move towards a global approach to all our work, not just assessment, but, more

importantly, policy; that the pillar structure worked against us and that we should make some organisational changes to compensate for this; in particular, that we should improve our inter-pillar co-ordination, possibly through the establishment of a co-ordinator charged to do this; and that we should improve our assessment and evaluation work—and one of the ideas would be to build a link between the SitCen and the internal services. This landed on Coreper's table and was probably going to take, as I say, 18 months to work through, but it landed on their table in late February, and on 11 March, of course, things changed. The Irish presidency, interestingly enough, concluded that many of these ideas should be pursued more rapidly, and there was a special European Council in late March, after the Madrid bombings, which very quickly endorsed a proposal by Solana to appoint a co-ordinator and invited Solana to come forward with detailed ideas for how you could make the link between us and the security services. Solana prepared a paper for ministers at the following European Council, which was endorsed, which went into some of the practical details about how to establish this link. The ideas were not terribly complicated but simply that the group should have a small presence in Brussels embedded within the Situation Centre, and that we would therefore be able to fuse inputs from internal and external services and we should use this to provide evaluations intended to assist policy makers. I would stress the point that the goal of this whole enterprise at Brussels level is to tackle only a small part of the problem: to tackle improving the information base that EU decision-makers and policy makers have available to improve decision-making at a European level. It is not intended to recycle back to the Member States information which they need for improving their own security or for improving their own policies to guarantee their security. It is intended to aid the Brussels-level function. Clearly certain policies that might be developed at a Brussels level have national implications in terms of their implementation but it is focused at aiding Brussels-level decision-making. As a consequence, it represents only a fairly small part of the whole counter-terrorism picture. The European Council agreed this basic concept and asked Solana in the semester (the six-month period) we are in at the moment to move forward with implementation and to report back in December. He will report in December that we have established the necessary links, information is flowing and reports are already being produced for Council bodies, though we will not take on the bulk of our staff until the New Year. That is how we have arrived where we are. During this process there has been a lot of extraneous interest relating to the question of operational co-operation between services. That is not our business in any way. Clearly we now have fairly extensive contact with the services and we have an impression of what is the level of their operational co-operation, but our function is unrelated to that. You can ask Mr de Vries yourself, but there is a stronger link to his work, in that certain policy activity in Brussels could, on the one hand, aid co-operation between the services, but could, indeed, on the other hand, actually hinder co-operation. You can imagine European policies that might facilitate data transfer which would facilitate the work of the services or which could conceivably make data transfer more complicated. You can pose him a question of how European action can help or hinder the operational co-operation, and he is conscious of the extent to which there is operational co-operation. It is his area more than mine.

Q153 ***Chairman:*** Thank you very much indeed. That has given us a very clear picture of what you do, what happens here, and you have really answered my first three questions. Could I just clarify that the new capability is the links that you are setting up and the new information flows, set up within the Centre, dedicated to counter-terrorism.
Mr Shapcott: Yes.

Q154 ***Chairman:*** That is fine. What special resources it would have is something that quite interests us.
Mr Shapcott: The link takes two forms, really: information, assessed intelligence from the services, and analytical expertise. Because we are not doing any operations, we are not doing anything complicated in a technical manner, our strengths are the quality of the analysts that the Member States choose to send to work here. On the basis of our experience in the external area, where we have been sent some very good analysts by Member States, we in fact interviewed analysts last week for these positions. It is their analytical skill, their experience that they have built up through working in the national services, plus the information which their services will send. I think it is important to stress that one of the attractions in working with the group is that we have a wide base. There are 25 Member States and some of them have two services in the group, so there are 27 services that will be providing information, and our analytical team should, I hope, be able to make good use of that information.

Q155 ***Chairman:*** Do you have any particular language problems across the number of people you have, the analysts here?
Mr Shapcott: The Counter-Terrorism Group has had a history of exchanging information in English and French, which is obviously helpful. The external services do not have a grouping and therefore have less tradition in terms of co-operating with each other, so it is a more complicated situation there. If

services send material in English or French, it is helpful, but sometimes that slows matters down, so we have to accept that if we want it faster we may have to take it in the original language and manage within our own resources.

Q156 ***Chairman:*** Do you have the resources to manage that?
Mr Shapcott: Yes.

Q157 ***Chairman:*** Could I ask about Europol and whether they see your reports and whether they are relevant to Europol?
Mr Shapcott: Europol is an interesting area. There have been discussions in the Council—you may have seen some reflection of this in press reporting—about the relationship between the various actors. Europol's strength is obviously its link into the police services and they have done some quite interesting post-criminal-event analytical work that flows from investigations. We will be very interested to receive information from Europol. We will, I imagine, from time to time produce joint reports for the Council. Clearly the Council bodies would prefer not to get four or five different analyses on a particular problem, so we are committed to working with Europol to produce joint reports where that is appropriate, but there will be some limitations. I think, also, just as in the national structures, if producing a joint report means you have to dumb down the quality of information needed in order to share it with a wider group then that is perhaps a disadvantage, so I think from time to time we will have to not share information directly. It is an area which is not fully resolved. I think it is correct that the Counter-Terrorism Group services operate, like many of these exchanges, what they call a "third-party rule", whereby information is shared on the understanding that it will not be passed on to a third party.
Chairman: Thank you very much. That is extremely helpful.

Q158 ***Lord Wright of Richmond:*** Could I ask a question about your sources of information. You have referred to diplomatic reporting. If I can be anecdotal for a moment, I remember, when I was ambassador in Saudi Arabia, that the EU embassies occasionally sent co-ordinated reports on the economic situation in Saudi Arabia, never, as far as I can recall, on the political situation. Are you now getting any sort of political analysis, for example, from Saudi Arabia, on the terrorist threat and on the political situation?—I mean, by combined embassy reporting addressed to you.
Mr Shapcott: Yes. I do not know how much it existed before I arrived in 1999 but it has become reasonably common practice for the bodies in Brussels to invite the EU Heads of Mission to submit a collective report. Obviously you are more experienced than me, but these are easier to do on less controversial subjects, so it is easier to get a Heads of Mission report out of Sudan on the situation in Dâfûr than it would be to get a Heads of Mission report out of Washington on developing Iraq policy, for example. And the bodies in Brussels are not themselves naïve: they ask Heads of Missions to do this where they know they are likely to get a good product. On terrorism in Saudi Arabia, I do not think they have done it, but Heads of Mission in some areas certainly have produced terrorism reports, so it is not as though terrorism is off limits. I think I have seen some from Indonesia, for example. Where there is less of a marked national interest and a strong common interest, it is clearly easier. Saudi Arabia I think is probably still a bit sensitive, because people have different perceptions and different furrows that they are ploughing. But I still think you would probably get something reasonable out of Saudi Arabia now.

Q159 ***Lord Wright of Richmond:*** Would those reports be copied to all 25 capitals?
Mr Shapcott: Yes.

Q160 ***Lord Wright of Richmond:*** I think you have answered the other questions I was going to ask, except the question of EU criminal intelligence policy. The Commission suggested there is a need for a common EU intelligence policy. What is the Council's view on that? Could an EU-level intelligence policy be developed that did not cut across the priorities of Member States?
Mr Shapcott: It is, first and foremost, more a question for Mr de Vries. I think you are all familiar with the fact that you are in a Council body where we are talking about co-operation between the Member States. I should stress that the exchanges to which I have referred are very much intergovernmental. There are no obligations on the part of the Member States to share this information; they do so voluntarily. I think across the street, between the Council and the Commission, there is a difference of emphasis. I would think that Solana's view is that, again, this is an area for the Member States to make the running, whereas the Commission want to push things along a bit more. I think everything is still a bit too embryonic, a bit too sensitive, to expect to be able to make rapid progress. I think it would be much better to build on the modest pragmatic co-operation that is under way before having an overarching policy document. Maybe it is sometimes a point of attack—and I know you are parliamentarians—but the existing work we have done has been done without any major policy documents, without any major fanfare. It has been pushed through pragmatically on the basis that it represents simply an

exchange of information, there is no intelligence activity by the Union. I just think that the pragmatic approach is likely to bear fruit more quickly.

Q161 ***Lord Avebury:*** We have been hearing about the principle of equivalent access in connection with the counter-proposals from the Commission. Do you think that is a principle which can apply to the sort of information you are dealing with?
Mr Shapcott: I have to keep stressing that we are not dealing with operational data, we are dealing with assessed intelligence—preliminary conclusions drawn on the basis of operational work to which we are not strictly privy—so I do not think our information really falls under that heading, quite frankly. Our information could be derived from one piece of operational work or it could be a composite of 20 or 25 pieces of operational work, but you do not know that, so there is a sort of firewall between us and the basic data. As I understand it, equivalent access really relates to access to the basic data, so I do not see it really applying in our area.

Q162 ***Lord Avebury:*** I was not actually thinking of it in those terms, I was thinking that if you distribute this information to the 27 countries, that it exists in retrievable form in the 27 countries and therefore the principles that apply to any other information which is held by the authorities in those countries ought to apply to the information which you have sent them.
Mr Shapcott: The notion which the Member States have accepted is that our information, whilst being EU information, is itself a composite of national information. The principle of originator control applies, so Member State A cannot grant access to one of our documents without the agreement of the other Member States which have contributed to it. Perhaps I have not really understood the question.

Q163 ***Lord Avebury:*** The question is whether this principle of equivalent access which is in the current proposals from the Commission would extend to the information which you have disseminated to the 27 Member States. From what you say, I gather it would not, because there is still some ownership of the information by the parent individual providers, so the short answer to the question is "No, the principle of equivalent access would not apply."
Mr Shapcott: I think so.

Q164 ***Lord Avebury:*** Unless the individual pieces of information were held in a separate form and that separate form was subject to the principle.
Mr Shapcott: Yes. I think I would return to the distinction between assessed/evaluated material and raw material. We do not have access to raw material.

Q165 ***Lord Avebury:*** Could I ask what you think about the sharing of information between police and intelligence services. Could you say what limits you think there should be on the exchanges of information.
Mr Shapcott: One of the interesting features of what we are trying to do is that we are trying to create a European model in an environment where there are 25 different national models. What we are doing does not look dissimilar, I suppose, from some of the analytical work being undertaken by JTAC in the UK; the concept being to try to pool all the available and interesting information about a particular problem. But it is true that that model is not a model which all the Member States can use: some have quite strong separations between their police and security service information. The country that springs to mind most clearly is Germany, which has anchored in its Constitution the notion of separation between the two types of work. These differing national modalities do represent a limit on what we can do, or result in limits on what we can do, but, more importantly, I think they do result in limits also between what is possible in the more operational areas. The sharing of information between the German security service and Europol is caught up by the national blockage on sharing between its security service and police. We will not quickly get over these national—"idiosyncrasies" trivialises them—these national differences, which will have a quite profound impact on European organisation. If you look at some of the policy documents, particularly since 11 March, they have talked about the idea of common databases, breaking down the limits on sharing. You can draw and design as much as you like at a European level but you will get tripped up by the national provisions. Some of these national provisions are not whims; they are the consequence of constitutional arrangements. It is clear that the Germans cannot internally produce a common database because of the restrictions on sharing between their entities. (*Brief off the record discussion*) In Germany, it is a very concrete constitutional obstacle and there are many Member States where it is the same. I was in one country where there had been a terrorist incident fairly recently and they were talking about trying to look at phone records and work out with whom their suspects had been in contact elsewhere in Europe. This intelligence officer said he needed a chart which told him how to get the answer to his question about which telephone number had been called, and this chart had 25 entries on it and it told him who he had to call in France, who he had to call in Belgium, who he had to call in the UK. It essentially showed 25 different ways of organising inquiries of this nature. In some countries this was very simple and in other countries it was highly complicated.

Q166 ***Chairman:*** Why could that not have been done through the Europol desk where they have fantastic charts?
Mr Shapcott: He could have put the question to Europol, you are right. The problem is that he was in the intelligence service and he would have to get his police force to do it and, he obviously had or thought he had other ways around it. But, even if you put the question to Europol, the national points of contact would run into the same problems. In one case they would go back and they would get the answer quite quickly; in other cases, you would need a *commission rogatoire* and even with a *commission rogatoire*, he said that in one or two Member States you never get the answer because they have constitutional legal provisions that prevented the sharing of that sort of information. There is quite a lot of broad-brush "Aren't common databases/isn't information sharing a jolly good idea?" and at the same time there are quite a lot of very, very serious obstacles. And those obstacles differ from State to State, which makes it even more complicated.

Q167 ***Chairman:*** Who is doing work on overcoming those obstacles?
Mr Shapcott: De Vries and the Presidency and the Council, the JHA Council, are grappling with this.

Q168 ***Chairman:*** Does anyone have primacy?
Mr Shapcott: No. Benjamin knows more about this than I do, but this is all Member State business, essentially.

Q169 ***Lord Avebury:*** If Germany is the only odd-man-out and their Constitution was the only factor that hindered a move which all the rest of the European Member States thought sensible, then there would be mechanisms behind the scenes for bringing some pressure to bear on them.
Mr Shapcott: There is a reflection underway in Germany as to whether they might change their own arrangements but they are certainly not unique. There are a number of other countries . . . The Nordic countries particularly have very strong concerns in the field of data protection. I think many are reflecting internally, but these are not difficulties that will be swept away quickly.

Q170 ***Chairman:*** Reflecting at different levels the seriousness of what they have to do. You have mentioned Nordic countries. I make no particular distinction between countries, but, in fact, some countries take the threat of terrorism far more seriously than others. Some are more or less in denial that it will affect their country.
Mr Shapcott: I think that is changing. I think the number in complete denial is diminishing, but the number where it is perceived as an existential issue is still not equal to 25.

Q171 ***Chairman:*** So too high.
Mr Shapcott: Yes.

Q172 ***Viscount Ullswater:*** In view of the impediments which you have identified, what is your view about the proposal from the Swedish government to simplify the exchange of this information between the intelligence and law enforcement authorities. Am I right in thinking it will have behind it a legally binding instrument?
Mr Shapcott: I am not, I must confess, familiar with the details of the Swedish proposal. I recall there is one, but it is focused particularly in the criminal area, I think—police information.
Viscount Ullswater: It is mostly police authorities, yes.

Q173 ***Chairman:*** Our specialist advisor outlines the proposal in this way: it is a fairly short paper with about 12 articles which says that not only local authority agencies but a range of other agencies need to exchange data or have access to data that may be held in other countries. It gives a long list of the different types of criminal offences—you are right there—but it includes terrorism, whereby information should be shared within 12 hours if asked. There is a "get out of jail card" in article 12 as well, that it is "too sensitive" or something like that, but essentially it is urging better exchange of data, not for evidential purposes but purely for intelligence purposes.
Mr Shapcott: I am not an expert—and even your next speaker is not an expert—but you probably need to go and ask people from security services or a number of security services who have direct experience. Many of these initiatives seem to be founded on the idea that the services are not doing any of this, and I am not sure that is correct. I think there is plenty of evidence which suggests that they are co-operating quite extensively. I am struck that on the day that Solana briefed interior ministers on what we were trying to do, he gave a short press conference and he was asked: "This is fine, but it is analytical. Why have you not come up with any proposals in the operational field relating to exchange of data, etcetera? This is not good enough. Why are they not co-operating more?" and it was interesting because that day there had been a five-nation arrest operation following up on the Madrid bombings, in which people had been arrested in five countries, acting on information obviously coming from the Spanish but also with extensive operations in those countries. He cited this almost as a rebuttal to the notion that there

was insufficient co-operation. I think with the proposal you have explained, much of the information will be shared already. I think the services have quite a high sense of responsibility in terms of information sharing. You ought to consider that we are now in an environment where parliamentary inquiries and post mortems are the order of the day, so, if there is an incident and it comes to light that someone has not shared some vital piece of information, that is going to reflect on everyone and I think services are therefore quite committed, where possible, to sharing information. The biggest difficulty comes from not perhaps appreciating the significance of the information that you have. That is what clearly tripped the Americans up. Sad to say, I do not think Europe has advanced enough really to have an easy solution to this. I think the risk of it being withheld for other less honourable reasons has diminished enormously. I think there is a high sense of commitment to work together.

Q174 ***Viscount Ullswater:*** Would I be wrong in interpreting what you are saying as that information at the lowest common denominator is widely disseminated? Or is it of a much better quality than that? Is there perhaps an opportunity of layering information, so that, although it might have equivalent access, it can only be accessed at certain times for certain reasons?
Mr Shapcott: There are some ideas. You might usefully talk to Interpol. I talked to the Director the other day who highlighted a method. They have a system whereby, when someone's passport is checked, you can go to an Interpol database and the Interpol database does not tell you why country A is interested in this person but simply tells you that country A **is** interested in this person: a red light goes off at a border control and you then have to follow up. That means that any intelligence sharing in relation to this can remain bilateral. People are not having to share multilaterally to feed a central database; they are feeding a central warning list. That is one way of getting round it. The other point I would make is that I do not think it is lowest common denominator. Bilaterally services are sharing solid, raw operational material. The Benelux countries have highly developed co-operative arrangements relating to cross-border surveillance; many countries have rehearsed arrangements for cross-border surveillance. I cannot remember if it is still in the Hague Programme, but in one of the early drafts of the Hague Multi-Annual Programme there were questions of facilitating surveillance and the notion that surveillance can go on uninterrupted across borders. Many countries have standing arrangements in place to deal with this. I think the services are sometimes caught in a situation of doing a lot of really concrete work, not being able for operational reasons to make a big issue of it, and, therefore, being exposed a little bit to people who assume, because they cannot see it, that there is nothing happening.

Q175 ***Viscount Ullswater:*** Would you say that the information that you are sharing between the 25 Member States is shared in the same way as you were describing Interpol information? Is it red lights, which you can then go on a bilateral basis to discover more about? Or is it that once you have put the information into the forum, that is it?
Mr Shapcott: I do not want to go into too much detail of precisely how we build the reports.

Q176 ***Viscount Ullswater:*** Maybe that was too sensitive a question.
Mr Shapcott: Looking at it from the other way, our end product is a bit like a JIC assessment: it is an evaluation intended for a fairly strategic level audience. I am sure Lord Wright will remember that you can have a JIC assessment that does not obviously look like it contains intelligence. An uninitiated reader might not read a sentence and conclude that beneath that sentence there is a piece of concrete intelligence, but, nevertheless, it is intelligent conclusions drawn from more fundamental material. You should think in those terms in how you regard our products. I think, for those reasons, it is fairly evident that we are quite a long way from the operational information.

Q177 ***Lord Wright of Richmond:*** One of the criticisms by the Franks Committee of the Joint Intelligence Committee of the Falklands was that we did not take adequate notice of press comment and other open information from Argentina.
Mr Shapcott: Our reports are all-source reports and quite a major part of our team is involved in mining open sources. We are beginning to use more and more technology to do that. It is becoming a more automatic process. Saudi Arabia is an example. I think it will not cause any stir to say that the Saudis are a little bit circumspect about how they brief their partners, but you can nevertheless get quite a good picture of the level of terrorist activity, the nature of terrorist activity, patterns within that terrorist activity, simply from open-source activities, because these attacks are reported, the details are known. You will not know anything about the work of the Saudi security forces necessarily to combat this, but you can nevertheless form quite a good picture of the activity and the characteristics of the activity without any intelligence at all, but it is nevertheless useful work. Open sources represent a significant proportion of our work.

Q178 ***Viscount Ullswater:*** Do you as an organisation have any arrangements for transferring data to third countries?
Mr Shapcott: By and large the Council has the necessary legal arrangements, but, at the same time, we exist for the purpose of supplying EU customers. We do not have a liaison function.

Q179 ***Viscount Ullswater:*** But the legal framework exists.
Mr Shapcott: If we had to, we could, in most of the obviously important cases.
Chairman: Could we move on to institutional structures now.

Q180 ***Earl of Listowel:*** Mr Shapcott, I think you may have answered to some degree in your introduction the questions I am going to put to you now, but, if you have further comments you would care to make,, it would be useful, I am sure. What is the Joint Situation Centre's relationship with the counter-terrorism co-ordinator, the Police Chiefs Task Force and Europol, and how do you see the co-ordinated role?
Mr Shapcott: From my perspective the Co-ordinator is a very important customer. Our work ought to be able to assist him substantially in his job. I think he can assist us, or he can assist the Council in our area. It is no good producing the most beautiful—as they are—intelligence assessments; I think the Council needs advice sometimes on what to do, so we see the Co-ordinator as an important catalyst in making sure that our work is well choreographed or integrated with the ongoing business of the Council. Where something novel crops up, if the intelligence suddenly reveals an issue which needs to become part of the business of the Council, then he should be an important actor in programming that, in making sure that advice is also available in tasking the various bits of the Secretariat to come up with some advice. Our experience in the Second Pillar is certainly that the Member States find assessments most useful when they are married up with some policy proposals, so we see him as having an important role in that sense. The Police Chiefs Task Force is less obvious. Certainly vis-à-vis Europol, the Member States are less settled in quite what they want the Police Chiefs Task Force to do. I think they have a somewhat clearer view of what they want Europol to do. As a consequence, we have had very little contact with the Police Chiefs Task Force. Europol, I have largely covered. I should say that justice and interior ministers gave Solana some very clear guidance, which was that they wanted a close, co-operative relationship to be developed between SitCen and Europol. He was tasked to do a number of concrete things: to make sure that an appropriate legal basis existed for the exchange of information; to make sure that properly protected links existed; and to make sure we had started establishing the managerial contacts necessary to result in due course in good contacts—and he has done all of those things. So we are looking forward to a close and productive relationship with Europol, although obviously I would record a a slight lack of clarity yet on the extent to which security service information would be shared with them. In terms of the co-ordinator's wider role, as the job title and the terms of reference suggest, I think the original conception was that this was intended as a measure to help compensate for the structure of the Union and this division into pillars. I think, since he has arrived, maybe partly through his own efforts, partly through a growing realisation of the problem on the part of the Member States, the relationships between the Council and the Commission are much closer than they were. I think you saw Jonathan Faull this morning, and I do not know whether he said the same thing, but we are gearing up to support the Commission as we move into production, for example. It had not been done previously. I think the contacts between the various bits of the Secretariat and the Commission are much more intense than they were. I think there are two reasons: (i) the fact that we now have a Co-ordinator and (ii) the Member States and the Commission are much more aware of the need to do this. I think there is an important task for him to fulfil vis-à-vis the Commission. I think there is an important internal task within the Secretariat General also to make sure that the connections are much stronger. I think that is happening. Papers being developed in the Second Pillar to look at the role of the defence instruments are now being worked together with officials from the Justice and Home Affairs area in a way which did not happen six or seven months ago. Again, it is not mono-causal: I think several things have resulted in that change.

Q181 ***Earl of Listowel:*** I think you have answered the last two questions I have for you, but I will put the first one to you and see if you have anything to add. How could the activities of the various EU bodies in the fight against terrorism involved be better co-ordinated? Is there scope for streamlining them?
Mr Shapcott: I think you catch us really in the middle of doing some of that streamlining. Part of the reason for giving the SitCen these responsibilities was to take assessment work out of several Council working groups, leaving those working groups free to do more work in the policy area. I think that is an example of some improvements already under way. Leaping to your next question, the Situation Centre has always been in the Secretariat. We have been quite careful, even from the beginning, not to formally have it in

the Second Pillar. We have played with Solana's double-hatting. He is the Secretary General; we are attached to his cabinet, so we are squarely in the Secretariat General. We are not exclusively a Second Pillar body. As discussion about our role has developed, Justice and Home Affairs ministers have said, "We don't know much about the SitCen and is that not something that works for Solana?" and we have said, "Come what may, in the future our goal is to work for you. We very much want Justice and Home Affairs ministers to be co-owners of this project; to control it, to the extent that their interests are the interests of the services which they supervise and are involved; and to be customers, quite clearly." I think we are getting there. I think we are persuading them. Solana has contacts with Justice ministers which he never used to have. I now go to a host of JHA Committee meetings which I would never have dreamt of a long time ago. De Vries as well. We are all trying to make sure that the interior ministries see SitCen as something that they own jointly and that works for them. So I think on that aspect we are getting there. The last point I would make is that Coreper is also trying to do its bit. It is the only sub-Council body which has this cross-pillar vision, and I think it is no surprise, therefore, that they decided they should have an enhanced co-ordination function on this issue. There have been various suggestions that there might be other cross-pillar bodies established to look at terrorism. I do not think that issue has gone away. I think what has happened is that Coreper are saying, "For the time being, we will do it, and we will consider in the light of experience whether something narrower but also cross-pillar is needed."

There followed a short discussion off the record

Chairman: I think we have probably come to the end of our questions.

Q182 ***Lord Avebury:*** I would just like to come back to what you were saying about the public domain material which forms a large proportion of the stuff that feeds into your analysis. Have you ever considered contracting out that function, say to a university? If I could give the argument for doing that. If that person collected together everything about terrorist activity that was on, say, BBC monitoring or the Dacca *Courier* or *Dawn* in Pakistan, etcetera, it would not only be available to users of your services but to a great many other people who might actually contribute extra information about the incidents concerned. If it was based in a public domain location such as a university, by the very fact of it being there you would generate a lot of information.
Mr Shapcott: Possibly. You would also reveal your areas of intelligence interest.

Q183 ***Lord Avebury:*** I am talking about public domain stuff, stuff that is in the newspapers or broadcasts.
Mr Shapcott: Even so, we have a list of countries of intelligence interest which drives our open source collection work as well as our requests for intelligence. Our contract with a university would immediately identify our areas of intelligence interest, for instance.

Q184 ***Lord Avebury:*** Unless you made it cover every country. After all, terrorist incidents are not confined to one or two countries now, are they?
Mr Shapcott: No, but I am not sure it is reactive enough. We are in a situation at the moment where we can fine-tune our trawling operation immediately. We have staff working 24 hours a day. We can leave the office at seven o'clock and ask them to pursue a particular angle and by six o'clock the next morning we will have the product of their research. I think that is a bit more responsive than we would get through an external operation. That is not to say we are not interested in having links to non-conventional sources. I would approach this from a slightly different angle, in that we have relationships with a number of NGOs which are quite valuable, especially in parts of Africa where most of the European intelligence services packed up and left 50 years ago: Dâfûr, for example—in fact, we rely quite extensively on NGOs for information, because no-one else is there. So we are not conventional in that sense. I had not, I must confess, thought of the model you suggest, but I think there are a couple of obstacles.

Q185 ***Lord Wright of Richmond:*** There is another model, of course, which is international institutes like the International Institute for Strategic Studies and Chatham House and the various French and German international institutes. I do not know whether you have had direct contact with any or all of them.
Mr Shapcott: A little bit. We are in a slightly awkward position at the moment, in that they often want to know more about us, and we have been trying to focus on our core job at the moment. There is much debate in Brussels at the moment about the External Action Service envisaged in the Constitution. At the moment we benefit in a rather passive way from the work of the Commission delegations. The Commission delegations produce reporting for the Commission in Brussels. Often this includes political reporting. It is generally shared with us. It is quite interesting and quite useful, but we cannot task them—the Commission do not like us to task them. In the future, if the Constitution is ratified, these delegations will become part of the European External Action Service and we will be in a position where we can task them, we can steer their activities, and that will be a major benefit. Similarly, with the

Member States' services, we are benefiting from what they choose to share with us, we are not tasking them. Clearly that would not be acceptable and that would not change, but with the External Action Service, from our perspective at least, there would be an advantage to being able to ask delegations to go and find out particular bits of information—through conventional diplomatic-type activity, nothing untoward, but at the moment we are a sort of passive beneficiary.

Q186 ***Lord Wright of Richmond:*** How many delegations are there?
Mr Shapcott: There are 140.

Q187 ***Earl of Listowel:*** Do you have any particular concerns about training across the European Union?
Mr Shapcott: I am not involved really. I do not have a view.

Q188 ***Chairman:*** May I, on behalf of the Sub-Committee, thank you very much, Mr Shapcott, for being so helpful in your responses to our questions, for giving us such a good view of the work of the joint Situation Centre. We have very much enjoyed meeting you and hearing what you have to say. We hope you will also enjoy reading our report.
Mr Shapcott: We will have to see.

Q189 ***Chairman:*** When it finally comes out. We hope it will be helpful to you. It may well be that you can use it in the future. Once again, thank you very much indeed.
Mr Shapcott: Not at all. My pleasure.

WEDNESDAY 3 NOVEMBER 2004

Present	Avebury, L	Listowel, E
	Harris of Richmond, B (Chairman)	Ullswater, V
		Wright of Richmond, L

Examination of Witnesses

Witnesses: MR GIJS DE VRIES, EU Counter-Terrorism Co-ordinator, and MS PATRICIA HOLLAND, examined.

Q190 ***Chairman:*** Mr de Vries, a very warm welcome. Thank you so much for coming to see us whilst we are in Brussels. We have had quite a long day. We have taken lots of evidence from a number of people—which has all been enormously helpful—to take us through hopefully to our conclusion and report, which eventually, of course, you will see and we hope you will find helpful. You have met all the members of the Committee. All that remains is for me to say that some of us have registered our interests in this particular matter. They are on a piece of paper there so I will not bore you verbally with what they are. I wonder if you would like to start with making a statement and then we can ask you questions in turn.
Mr de Vries: Thank you very much. May I, first of all, thank you for the opportunity to meet. I have been exposed over the years to various products of the work carried out by your Select Committee and I have always admired the high quality of it. I believe the House of Lords is a model of its kind among the parliaments of Europe in taking the European Union seriously and devoting time and attention to scrutiny of its actions. I believe that is extremely important. I believe we have in Europe a joint responsibility at national and European level to make sure that our citizens are properly represented and that scrutiny is carried out. That cannot just be the task of the European Parliament: even though it has a crucial role to play, it is equally important that national parliaments play their role fully. Let me thank you very much for the opportunity to contribute a little bit to your discussions and your analysis of what we do and do not do in this field.

Q191 ***Chairman:*** Thank you for those very kind remarks.
Mr de Vries: They are not mere politeness. Both as a member of my Government and as a Member of Parliament, I have had a great deal to do with the reports you have published over the years. Not to go over ground with which you undoubtedly are already familiar, I would like simply to say that the role of the Union in the field of counter-terrorism has taken shape mostly after the attacks in the United States on September 11 and has received a clear new impetus as a result of the tragic attacks in Madrid earlier this year. The role of the Union in the field of counter-terrorism is an important one, a growing one, but a limited one. The key role in this work is still, I believe, in the responsibility of Member States. It is a Member States' responsibility. Member States are in charge of the operational dimension in terms of the functioning of police forces, judicial authorities and security and intelligence services. The role of the Union, in my view, is complementary to the role of Member States, and it consists in helping Member States and their agencies work together across borders to tackle jointly what is increasingly a cross-border phenomenon. I think there is there a classic role for the Union in terms of subsidiarity, subsidiarity upwards; that is to say, the role of the Union is one of supporting the Member States in this particular field. Of course the Union has equally some competences that have been granted in the Treaty and of course they will have to be carried out. Increasingly, I also see that the role of the Union is taking shape in the external field; that is to say, the mainstreaming of counter-terrorism in external relations is increasingly becoming a reality, even though a lot of ground will still have to be covered. I am happy to address any questions you may have on that point, but I merely wished to highlight, as I have seen some of your questions, the importance of the external dimension. We cannot fight terrorism even as a European Union unless we do so in close co-operation with the Americans and with others across the world. That dimension, I believe, is absolutely critical to the success of our efforts.

Q192 ***Chairman:*** Thank you very much indeed. You have probably answered my first two questions, and certainly you have explained why the need for your post was established, but I wonder if you could tell us how it was established. I would find that quite interesting.
Mr de Vries: It was established by the Secretary General High Representative, Javier Solana, who felt that it would be useful for himself and for the Council if he were to be assisted by someone who would concentrate on the co-ordinating work, notably within the Council, which is essential if we are to be effective. Perhaps I may give one example. The fight against the financing of terrorism is something which

touches upon the competences of the Ministers of Finance, obviously, and the ECOFIN Council, for example, in terms of fighting money laundering. That is a classic First Pillar job. Then it touches upon the competences of the Justice and Home Affairs Council in terms of the law enforcement aspects of the fight against the financing of terrorism. But it equally has to do with the work of our foreign ministers; for example, in discussing with the Gulf Co-operation Council how third countries could reduce financial contributions to terrorist-related activities inside the Union. Those three councils therefore have to work together. That is an element of co-ordination which I hope to help put into place. That is one example of the work that I am doing. I am looking also of course at co-ordination inside the Council Secretariat. I am looking at the implementation of the decisions reached by the Council. To keep an overview of all the instruments at the EU's disposal was explicitly requested of me, and, as the European Council in June indicated, the EU is also interested in giving sufficient visibility to its role in this area, both inside the EU and outside, so that is also part of my duties.

Q193 ***Chairman:*** If it is not too impertinent a question, did you have a job description? That is very simplistic, but were your duties, roles and responsibilities written down? Are they written down anywhere?
Mr de Vries: You will find in the conclusions of the European Council in March and June relevant paragraphs. We could certainly provide you with those.

Q194 ***Chairman:*** That would be very helpful.
Mr de Vries: Indeed, the Secretary General has, of course, as I support him and am a collaborator here in the Council Secretariat, defined what he expects me to do.

Q195 ***Chairman:*** I simply ask—and I do hope you do not think that I am being impertinent—because of the plethora of various people involved in the counter-terrorism arena. It is good for us to have a clear idea of where things sit. You have talked about some of the priorities that you have been undertaking since you took up your post. What are the main changes you feel you have been able to make?
Mr de Vries: First of all, anything that a co-ordinator does, I believe, ought to be seen in the proper context. There is no new decision-making capacity that has been created when this post was created. Decisions are in the hands of the Council where they should be. Perhaps I might try to address the question of what the Council has done in the meantime, to which perhaps the co-ordinator has contributed to some extent. The Council—and I believe it was a very good initiative of the Irish Presidency—has agreed a multi-annual plan of action. I believe that is an important instrument because it provides predictability to the work of the Union, and also to our national parliaments. I know from my own work in my national parliament that we at the time were often slightly bewildered by a seeming lack of clarity about what the EU was about to do in a particular issue area. We now have a road map indicating what will be done in the Dutch Presidency, the Luxembourg Presidency and the British Presidency. Any parliament wanting to do so could take that and plan its own activities of scrutiny accordingly. I have already thereby touched upon the importance of the timetable that is involved. We are now able to measure whether we, as a Union, do measure what the Council committed us to do. Thirdly, there is in the conclusions of the European Council in June a set of priorities. The plan of action is vast. It encompasses many measures. Clearly priorities are needed. The European Council has identified at least five: information sharing; the financing of terrorism; protection of critical infrastructure; the civil protection; and mainstreaming of counter-terrorism in external relations. On the latter four, it has commissioned proposals which are currently being prepared. The Commission has issued, as you know, its four communications. I am assisting the Secretary General in drafting his response to at least two of these papers, on financing and on external relations. So we have basically our road map in place. We have also looked at the functioning of the Council. Coreper has agreed to assume an active role in monitoring the work in various Council committees. That perhaps jumps slightly ahead to one of the questions you might wish to discuss later, but Coreper has said that it would pay close attention to the implementation of the conclusions of the European Council in March and June. So that is an additional co-ordinating mechanism which is now in place, and I have tabled some papers on implementation to CATS, and also, to the COTER Committee, implementation of the work of the Union in the legislative field but also in terms of mainstreaming our counter-terrorism concerns in our development policies, assisting thereby third countries to upgrade their capacities.
Chairman: Thank you very much indeed.

Q196 ***Lord Wright of Richmond:*** It sounds from what you have said as though your role is a developing one; that is to say, that there is scope possibly for widening it or increasing it. Do you see a role in co-ordinating operational questions on counter-terrorism? Do you expect to have a role—perhaps you do already—in representing the EU in international fora?

Mr de Vries: First of all, my role is that of assisting the Secretary General, Javier Solana, and it is therefore up to him whether he feels I should take on any additional activities. Of course, all that he and I do must be firmly within the constitutional framework of the Union, respecting the competences of the Council—I have already mentioned that—and respecting also the competences of the Commission. That is self-evident, but I am afraid sometimes it has to be emphasised. Operational work in the field of counter-terrorism, as I have mentioned, is Member States' responsibility and therefore it is perhaps best for the Union not to create expectations that the EU or any of its functionaries could not meet. We have to be clear about what the Union can do. We equally have to be clear, I feel, about what it cannot or should not do, so that the public has a clear image of possibilities but also the limits placed on the work of the Union. In operational terms, the role of the Police Chiefs Task Force is one of the issues which the Council is currently debating. Some Member States would like it to play a more active role in co-ordinating operational work in the field of counter-terrorism in its law enforcement dimension. That debate has not finished, and I cannot predict its outcome. Of course, in the new EU Treaty, assuming it will be ratified, there is a reference to a committee that ought to co-ordinate the operational work of the Union but it would obviously not be for the EU to anticipate the entry into force of the treaty before the people have spoken.

Q197 ***Lord Wright of Richmond:*** I am sorry, could I just reveal my ignorance, does the draft constitutional treaty refer to the co-ordinator?
Mr de Vries: No, it does not. That position was created by Mr Solana subsequent to the negotiations about the EU Treaty. As to external representation, that is the role of the presidency and of the High Representative, and, to the extent that they feel it useful to call on me, I am at their disposal. To be specific, Mr Solana and the presidency have invited me to go to Moscow tomorrow to discuss with the Russians to what extent we might be able to improve counter-terrorism co-operation between the Union and Russia.

Q198 ***Lord Wright of Richmond:*** Interesting.
Mr de Vries: But I do that, obviously, at the invitation of the Secretary General.

Q199 ***Lord Wright of Richmond:*** There has, I gather, been some criticism from the European Parliament's Civil Liberties Committee about the arrangements for the Co-ordinator in terms of accountability and the weakening of the Community character of the Executive. They have called for greater parliamentary scrutiny of your activities and a review of your link with the Commission. Could you tell us what your reaction is to this criticism?
Mr de Vries: In purely legal terms, again I am a special adviser appointed by the Secretary General in the Council Secretariat, which means that accountability is to the Secretary General and his accountability is to the European Council. In formal terms, that would be the answer. Having said that, I am, of course—as indeed is the Secretary General—prepared to answer any questions that the European Parliament might have. I have now visited the European Parliament three times and engaged in discussion with its Foreign Affairs Committee once and its Civil Liberties Committee twice—indeed, Mr Solana regularly appears before the European Parliament. I have also accepted an invitation to address the Conference of European Affairs Committees of National Parliaments, and another invitation to address a conference of the Committees of Justice of National Parliaments organised by the Dutch presidency in The Hague not too long ago. So I am, of course, available for these contacts, but in formal terms the Secretary General is responsible. The Commission, of course, has an important role to play. There has been some discussion, as you know, whether the co-ordinating role should be invested with the Commission or in the Council Secretariat, and the balance of opinion in the Member States was that, in view of the nature of counter-terrorism, this role was best created within the Council structures. Co-operation between myself and the Commission is excellent—with Mr Vittorino, Mr Patten, Mr Nielson, and I look forward to a similar close co-operation with the new Commission.

Q200 ***Chairman:*** That decision was made by Council.
Mr de Vries: The decision was made by the Secretary General.

Q201 ***Chairman:*** Yes, originally.
Mr de Vries: And it was confirmed by the European Council.
Chairman: Thank you.

Q202 ***Lord Wright of Richmond:*** Mr de Vries, one supplementary question, a rather political one: you referred to co-operation with the Unites States. To what extent since September 11 has there been any discussion with the United States about what they call the "war against terrorism" and the political principles that lie behind that? Have you been involved in such discussions?
Mr de Vries: Notwithstanding the political differences within the EU about Iraq, there has been a lot of practical co-operation with the United States, ranging from our joint determination to strengthen the role of Interpol (for example, in monitoring what

happens to lost and stolen passports: both the EU and the US have agreed to share information with Interpol about what happens to these passports—a critical component of our fight against terrorism) to the fight against the financing of terrorism, where there is a lot of practical co-operation and information exchange across the Atlantic. Earlier this year, it was decided to create a policy dialogue on border and transport security—a joint initiative: on the US side, Homeland Security, the State Department and the Department of Justice, and on the EU side, the Council and the Commission, with the Presidency of course involved. The idea of that dialogue is to anticipate potential hiccups in transatlantic relations. The lesson was drawn on the basis of our experience at the end of last year when the United States entered into discussions with several European Union airlines about transatlantic passenger traffic. The feeling was that a little bit more advance warning might have facilitated those exchanges.

Q203 ***Chairman:*** This has exercised us as well.
Mr de Vries: Similarly, on the question of container security, the United States originally approached several EU Member States bilaterally and subsequently learned that container security is part of Community competence and therefore the EU simply had to be involved from a legal perspective. We have ironed out these questions, but the dialogue is intended to allow us to exchange information about these issues before they reach the point where perhaps they may become more difficult to manage. We have, therefore—to answer your question—not directly engaged in the slightly philosophical discussion about whether the fight against terrorism ought to be called a war or not. There are different opinions about that question inside the Union and, indeed, in the United States, and we felt it might be more appropriate to focus on practical issues rather than on this admittedly very important political question.

Q204 ***Lord Avebury:*** Could I ask about something you said when you were describing you priorities and you mentioned the way in which you tackle the funding of terrorism through contributions made to organisations operating in third countries. This is a long way away from anything we can influence directly. I was wondering whether that co-ordination of the attempts to reduce the contributions to terrorism in third countries extends to an examination of the way in which Madrassas, in countries of South Asia in particular, are fomenting a climate of hatred which itself acts as the seed-bed for terrorism. Is this a matter that the priorities you describe embrace?
Mr de Vries: To the extent that the Council of Ministers identifies these questions, yes, because clearly one needs political guidance. This is a political discussion. I have just returned from a visit to Indonesia with the Troika, where the new Indonesian President emphasised strongly the importance of investment into the Indonesian educational system in the framework of a discussion about counter-terrorism. I believe that indicates that at least the Indonesian authorities are keen to offer sufficient high quality education so that the Madrassas do not *de facto* become an alternative to the educational system. We try, as a Union, in our relations with third countries to call their attention to, for example, the need to ratify and implement the UN Convention against the financing of terrorism. Many countries have not yet signed or ratified or implemented that Convention—indeed, two EU Member States have still to ratify this important Convention. I mention this because in our contact with third countries we emphasise the need to work closely with the UN. That implies ratification and implementation of all 12 UN conventions against terrorism, including the financial one. We are equally exploring with third countries how they can crack down on money laundering; how, for example, they can create financial intelligence units. In our discussions with Morocco, for example, it became clear that the Moroccan authorities would welcome EU assistance, technical assistance, to build their financial intelligence unit. We are now creating a network of these FIUs inside the European Union and extending that network to third countries, so we are trying to address a number of aspects of the question of the financing of terrorism in our relations with third countries, the role of Madrassas being one of them but not the exclusive focus.

Q205 ***Lord Avebury:*** I am very glad to hear what you say about SBY's[1] announcement, because I think what he says is of general relevance: it applies not only to Indonesia but also in Pakistan and Bangladesh. I would have thought one aspect of the struggle, fight, whatever you like to call it, against terrorism would be, as SBY has commented, diverting young people in these countries away from the Madrassas, where they receive this kind of hate indoctrination, and into a conventional education. Maybe one of the components that we should be promoting if we are looking at the funding of terrorism, is not just the negative aspect of producing the money that is flowing to the Madrassas, but increasing the positive amounts that goes from the European Union and other donors towards the conventional educational systems in these countries.

[1] President Susilo Bambang Yudhoyono.

Mr de Vries: We are at the moment looking into the general question of possible causes of recruitment. This question is certainly very high on the list of points to be addressed.
Lord Wright of Richmond: Good.
Chairman: Thank you.

Q206 ***Lord Avebury:*** Good. What do you think are the main obstacles to the co-ordination of counter-terrorism activities in the EU? What are the steps you think might be taken to overcome them?
Mr de Vries: There are perhaps some steps that could be taken. They are, I feel, primarily the responsibility and the competence of our national governments. First, it is of critical importance that decisions that are reached by the Council are implemented properly and in timely fashion by all Member States. Our record is patchy on this implementation question. Quite often it happens that Member States are finding it difficult to implement EU decisions in time. When the Commission, to the extent that its powers allow, requests Member States to report on implementation, these reports often come in late, therefore there is quite a bit that we could do to make our work more effective by making sure that decisions reached become decisions implemented. Secondly, to be able to co-ordinate the Council's work effectively at European level, it is of great importance that there is sufficient co-ordination at national level. This, of course, is not for Brussels to decide. The EU does not have competence to immerse itself in national co-ordinating mechanisms. That is for each Member State to decide according to its own constitutional tradition, but it is very important that it should happen. We are currently conducting a peer review at the instruction of the Council into how Member States organise themselves domestically in the fight against terrorism. That is therefore not a legislative exercise, where the EU is about to impose or decide things on behalf of Member States; it is comparing experiences, trying to identify best practices, and therefore offering, hopefully, some ideas that countries could take on board when addressing the question of internal co-ordination.

Q207 ***Chairman:*** What about those Member States who do not feel that taking counter-terrorism responsibilities on board is the major part of their programme—indeed, those who feel that it is not really up there with some of their more important internal concerns?
Mr de Vries: The European Council has now twice addressed, very much in detail, the role of the European Union. In the March conclusions and in the June conclusions there were extensive chapters devoted to what our most senior leaders feel should be the role of the European Union. It is therefore now up to the European Council and the Council in general to implement those decisions. Again, decisions reached should be decisions implemented. Therefore, I hope to report to the European Council in December about implementation, as has been requested of me, and it will then be for our political leaders to draw the consequences.

Q208 ***Chairman:*** Your peer review will find out whether there is a patchy take-up of implementation, if I may put it like that.
Mr de Vries: Yes, there is. The European Arrest Warrant, for example, has not yet been implemented by one Member State: Italy, as you know. There are eight Member States that have not yet implemented the framework decision on joint investigation teams. I mentioned the UN Convention against the financing of terrorism and I should also mention perhaps the three protocols that the Council has passed to strengthen Europol. One of the protocols would allow Europol a more effective role in the fight against the financing of terrorism. Another protocol would allow third countries, such as the United States, to work more closely with Europol. But, again, these three conventions have not yet been ratified.

Q209 ***Lord Avebury:*** I am just wondering if it would be possible for you to give us a note of the names of the Member States which have not implemented particular EU measures.
Mr de Vries: It is, I believe, the intention of the current Presidency to report in more detail to the European Council, and, with your indulgence, I would like to pass your request on to the Presidency.
Lord Avebury: Thank you.

Q210 ***Chairman:*** That would be extremely helpful.
Mr de Vries: The Irish Presidency, as you know, in June did indicate what the state of play was at that time.

Q211 ***Lord Avebury:*** It might have a salutary effect if you did a bit of naming and shaming. Do you think it would help if there were some enforcement machinery for Third Pillar measures?
Mr de Vries: If our record in the classic First Pillar is any guidance—and there are significant differences between this work and First Pillar work—the answer should be affirmative. The new Treaty allows, first of all, for qualified majority voting instead of unanimity in the fight against terrorism, which should have a beneficial effect on the quality and speed of decisions in general. It allows the Commission the task of taking Member States to court in appropriate circumstances and it allows the European Court of Justice the right to compare Member States' records with the Treaty. So, yes, I believe that would be

helpful, but at the end of the day implementation requires political will, and there is no substitute, I believe, for that. Even with the best possible legal machinery to secure implementation, there will still be the need for political accountability and therefore for a role of national parliaments.

Q212 ***Viscount Ullswater:*** Of course what you say is entirely correct. Do you see any warning signs, in the Council of Ministers who agree these decisions and these protocols, that there is going to be any hold-up in implementation? You say that there needs to be the political will, but the political will has already been given through the Council of Ministers to implement it, I presume, and then you say there appears to be a lack of political will when it leaves the Council of Ministers. Do you see any warning signs?
Mr de Vries: Perhaps I have not made myself entirely clear. I notice that, notwithstanding the political will as expressed in the Council decision, implementation by national administrations seems to take more time than was originally foreseen when implementation deadlines were fixed. I am not sure that indicates a lack of political will to implement. On the other hand, it might be good if the political will that was behind the original decision could be mobilised more effectively to secure implementation.

Q213 ***Chairman:*** You may not be able to answer this, but when the Council is coming to a decision that produces the political will, there will be Member States who will know that they may have difficulties—and I think particularly of the new States, those who do not have the wherewithal to implement things fairly quickly—they may not have the resources. How will that work? They make the decision and they say, "Yes, yes, we will do it," but, scratching heads, perhaps: "We will say yes in the Council but we know this is going to be difficult to implement."
Mr de Vries: With your permission, I am not sure the dividing line is strictly between the old and new Member States.

Q214 ***Chairman:*** I am sure you are right. I know you are right.
Mr de Vries: On some issues, the implementation record of our new Member States is actually demonstrably better.

Q215 ***Chairman:*** I retract my question!
Mr de Vries: That is not across the board, but it does happen. But, to open a bracket, the Union, the Commission in particular—and this is not on the implementation question but on the more general question of administrative capacity—does give quite a bit of aid to the new Member States to help them to continue to adapt their administrative systems; for example, in order to allow them hopefully one day fully to join the Schengen arrangements. The Commission has earmarked about €1 billion for the period 2004–06 in various categories to help the new Member States continue their reform process and their process of administrative restructuring.
Chairman: I am straying into Lord Listowel's area, and I do apologise, but thank you for that.

Q216 ***Earl of Listowel:*** I would like to ask a few questions on the institutional arrangements, Mr de Vries. In its declaration of 25 March 2004, the European Council called for new institutional structures to be put in place. Has this happened?
Mr de Vries: It has to the extent that Coreper, after discussing various options, has decided to take upon itself the role of overseeing the various Council bodies more in detail. So Coreper has strengthened its own role in co-ordinating among various Council bodies.

Q217 ***Earl of Listowel:*** To what extent is there a need to increase national capabilities to combat terrorism as opposed to strengthening EU structures?
Mr de Vries: I am not entirely certain that one would need to see the strengthening of national structures in opposition to the strengthening of EU structures. My experience would suggest that, for the EU to be effective, we need effective national governments, and that, therefore, a well-functioning national set of institutions and structures is a *conditio sine qua non* for a proper functioning of the European Union. I see the model of the Union bottom up rather than top down. The Union cannot be effective if Member States somehow find it difficult to be effective.

Q218 ***Chairman:*** Can Coreper co-ordinate this work effectively, given its many other responsibilities?
Mr de Vries: It has felt that that was certainly among its responsibilities and it has decided that it wants to devote more special attention to the field of counter-terrorism at regular intervals. Of course this does not have to happen during every weekly meeting of Coreper, but during each presidency Coreper will focus repeatedly on the counter-terrorism agenda. That Coreper feels can be achieved, and my sense is that it is right in assuming it can.

Q219 ***Chairman:*** So you are confident that it can take on the extra work.
Mr de Vries: So far indications are that it can. But Coreper itself has recognised that it would have to review its own functioning after a certain amount of time.
Chairman: Thank you very much.

Q220 ***Earl of Listowel:*** I think you may feel that you have answered much of this question, but if you have additional comments to make I would appreciate them. What do you see as the respective roles of Europol, SitCen and the European Police Chiefs Task Force in the fight against terrorism. How can their activities best be co-ordinated? Should the task force be brought within Council structures?
Mr de Vries: Your last question requires a political judgment which I feel is the responsibility of the Council. I have my private opinion about that but I think this is clearly an institutional question, where the Council should take its responsibility. The Presidency is preparing a Council decision on this very issue, hopefully to be reached before the end of the year. On Europol, Europol's role is to collect and analyse criminal intelligence to support Member States' law enforcement agencies in their work. Its caseload, as you will have noted, has gone up significantly, about 40 per cent, I believe, in its latest Europol report. Eurojust's caseload has gone up by about 50 per cent. Clearly both bodies are beginning to spread their wings, even though both would indicate that they still have quite a way to go. SitCen's role, of course, is related to the functioning of our security and intelligence agencies and does not have a law enforcement focus.

Q221 ***Lord Wright of Richmond:*** If the Chairman would allow me to say this: you made reference to your personal opinions and I do not think we have said to you, as we have said to all our other witnesses, that if at any point you want to go off the record you would be very welcome.
Mr de Vries: Thank you very much.

Q222 ***Chairman:*** You would indicate if you would like to do that.
Mr de Vries: Thank you.

Q223 ***Earl of Listowel:*** The March declaration called for the further development of the relationship between Europol and the intelligence services. Has this taken place? You have already touched on this.
Mr de Vries: It may perhaps still be a little early to tell because Europol is rebuilding, reconstituting its counter-terrorism task force. That should be the focal point of that connection your question alludes to. I do not think that process has finished—they are right in the middle of it—so it may be easier to address that question in a few months' time.

Q224 ***Earl of Listowel:*** There seems to be a proliferation of groups within the EU concerning counter-terrorism. Is there scope for streamlining them?
Mr de Vries: To the extent that streamlining can be achieved, there is, as I indicated, a role for Coreper and I hope to contribute through my own work to the information exchange among various Council bodies. There are two bodies that focus exclusively on counter-terrorism. One is COTER in the external field and the other is the working group on terrorism in the old, current Third Pillar. There is reason for the existence of these groups. Member States have on occasion discussed whether a merger of COTER and the Terrorist Working Group would be a step forward. I detect quite a bit of scepticism—after all, the two do have a different focus and they do link up, if that is correct English, with different departments in Member States. Even if they were to be merged, the question would still have to be addressed how to link with these respective national departments. The solution reached at the moment is to have the two join forces on occasion; for example, with respect to a subject which is clearly cross-pillar in nature, such as recruitment. We have to address some recruitment questions inside the EU but we equally have to look at recruitment in third countries and draw lessons accordingly.
Earl of Listowel: Thank you.

Q225 ***Viscount Ullswater:*** Are you saying that, in your view, the existence of the Second and Third Pillars are not detrimental to the role that you play as a co-ordinator?
Mr de Vries: I am not a great fan of the pillars. Indeed, under instruction from my former employer, the Government of the Netherlands, I have worked during the Convention to eradicate the distinction between the pillars as much as feasible, because there are differences. My point is perhaps more that the ministers of justice have a very important role to play in the fight against terrorism, so do the ministers of the interior, and there is also a role for the ministers of foreign affairs. However one organises oneself at European level, one still needs the political and administrative involvement of these three sectors of national government. Regardless of how one organises oneself in Brussels, you need to link up with these three important domestic players. To that extent, I think they will all have to remain involved. I am not sure it has to be done through a legal structure at EU level which distinguishes, as the current situation does, between Second and Third Pillar to the extent that we currently do. Of course the external field will always remain different from our EU responsibilities. There is no doubt about that.

Q226 ***Viscount Ullswater:*** Perhaps I could ask you about an intelligence policy. Is there a case for an EU intelligence policy? What role could you as the Co-ordinator play in its development if you felt it was necessary?

Mr de Vries: Our prime ministers have looked at the role of the Union in the field of intelligence and felt that the best approach would be bottom up rather than top down. Rather than create a Euro CIA, they felt it was best to assist the national security and intelligence agencies in their activities across borders. I believe that priority was justified, a priority on working with the existing mechanisms rather than creating new EU institutions. It was justified because debates about institutions in the Union tend to last a considerable period of time, and we do not have that time in the fight against terrorism. We have to work with what exists and assist those institutions to do their job as best as possible. That means that the operational work will remain the prerogative of Member States when it comes to intelligence co-operation—and I am talking now about the security and intelligence services. The role of SitCen is to analyse information and to provide the classic helicopter view which now, fortunately, will be possible because of the joint input from the security and intelligence services—so that will have a view of the threat that is not only EU based or non-EU based, but combines the two perspectives.

Q227 ***Viscount Ullswater:*** That brings us neatly to questions about the exchange of data. A number of principles have been suggested to facilitate the exchange of police data between national authorities in the EU, in particular the principle of equivalent access and the principle of availability. Do you think these proposals will be of assistance, and how can data exchange for counter-terrorism purposes be improved in the EU?
Mr de Vries: The American counter-terrorism ambassador, Cofer Black, has said that, in his view, the name of the game is changing, and that the "Cold War focus", as he puts it, not to share information has gradually to change, and that the sharing of information becomes much more important as we are trying to address the current phenomenon of Islamic terrorism. That is his view. The Union has perhaps still some legal hurdles to take to allow for more cross-border exchange of "information"—which is wider than the technical term "intelligence". The Commission has issued a communication recently on enhancing access to information by law enforcement agencies, in which it has indicated the principle of equivalent access but has also highlighted the need for additional work to be done before this can be made more concrete. We have notably to address the question of data protection. We have different data protection regimes relating to different agencies. Europol has its own, Eurojust has its own, the Schengen system has its own. They are not easy to change—you need unanimity to do that—so the Commission will be considering a framework proposal to allow the Union to have an overarching data protection approach. The PNR debate in the European Parliament has clearly indicated the political sensitivity of this question and I believe Member States are acutely aware of this.

Q228 ***Viscount Ullswater:*** Perhaps that leads neatly on to the other side of that, which is calls that have been made, I know, for enhancing the interoperability of, I think, Member States' databases rather than EU databases. Do you see that as the next step or a parallel step, or do you see it as not being a useful step?
Mr de Vries: Again, I think it is probably too early to tell, because there are lots of knotty legal problems that would have to be addressed. Conditions of access, for example. Who would have access to these data? Under which conditions? How would the privacy of the individual be protected? These questions take time to be addressed and the best way forward, I think, is for the Commission to take its responsibility under the Treaty and a draft communication as it has indicated. Meanwhile, there is a separate but related question which the Council could address and that is information provision to Europol and Eurojust. Both bodies are doing better than a few years ago, but they still do not have a complete picture of all cases in Member States involving terrorism. There is a proposal before the Council according to which Member States would commit themselves to give all relevant information about investigations and court cases concerning terrorism to both Europol and Eurojust. That, therefore, does not involve a shift in responsibility or in authority or in competence, but it would allow Europol and Eurojust to have a much fuller picture of what is happening in Member States, so that they are better able to connect the dots and to compare experiences and to draw lessons. That could be done regardless of the previous issue of exchange among national databases. That would already be a step forward. A proposal is before the Council.

Q229 ***Viscount Ullswater:*** Is there a satisfactory framework for data protection in the Third Pillar? You indicated the difference in the many institutions where they have a difference. Do you feel that it provides an adequate level of protection?
Mr de Vries: The data protection regime in the Union is a First Pillar based regime. It does not extend to police co-operation—nor does the Council of Europe Convention, for that matter. We need to consider what kind of adaptation might be necessary for these mechanisms to be extended to the Third Pillar. It is clearly an issue that many people feel very strongly about and therefore has to be addressed at the political level.

Q230 ***Lord Wright of Richmond:*** I would like to put a question to you about British involvement in counter-terrorism. Speaking for myself, a conclusion I would draw from the evidence we have heard today is that it is very much in Britain's interest to play a full and co-operative part in all these various co-ordinated mechanisms of counter-terrorism. If you were invited—perhaps you have been—to address a Euro-sceptic audience in Britain, what would you pick out as the main advantages in the counter-terrorism exercise? I am sorry not to have given you notice of that question.
Mr de Vries: No, no, it is an extremely important question. Indeed, it is a question that is of great relevance to many countries of the Union where similar audiences exist. I base my own work on two ... the word "pillars" cannot be used in this context—two truths that I hold to be self-evident. First, that the fight against terrorism requires our national governments to use their national agencies to the best possible effect, but, secondly, that that necessarily includes international co-operation. This type of terrorism is international in nature. Let me now give you my personal view on the record: I believe government ought to be structured according to the dimensions of the problems that our citizens want to be addressed. If a problem is local in nature, then clearly it is for local governments to look at; if the problem can be confined or is confined to a Member State, a country, it is for its national government; but if the problem is both domestic and international, we need a proper mix of effective national government and effective European government. That is the basis on which I believe we ought to work, pragmatically looking for appropriate mechanisms that correspond to the nature and scale of the threat. I believe the United Kingdom is playing a full part in this important field. Many countries recognise the experience of the United Kingdom in many years of dealing with tragic circumstances in the United Kingdom and, of course, in Northern Ireland in particular. I believe the United Kingdom is playing a full part and I very much hope this type of logic will appeal to our citizens across the Union—indeed, if you look at the Eurobarometer, there is every indication that this type of logic is being embraced by the citizens of Europe, who clearly believe that this is an area where the EU, within the limits of its competences, ought to play a role.

Q231 ***Earl of Listowel:*** Mr de Vries, following on from that may I press you a bit further on the idea of an EU intelligence policy. Would it be possible, without setting up a separate intelligence service for the EU, to set a sort of agenda for the European Union to recognise the risks that we all face within the European Union, and to set priorities within those risks, so that we could work better together to combat these risks? Perhaps that is already what is being done. That is my understanding of what an EU intelligence policy might be.
Mr de Vries: At the moment—but you have, I believe, extensively discussed this question with William Shapcott—the decisions reached allow for the Situation Centre to provide integrated threat analysis to various Council bodies and to the Secretary General, so that our work can be better informed. That in itself is a very significant step forward. I certainly would not have predicted two or three yeas ago that the governments of the Union would agree to such a step. They have. Perhaps it is best now to gain some experience with this new set up, and, indeed, also to encourage Europol to play its full part with respect to the more criminal, more law enforcement related questions of intelligence co-operation. If the need arises to go further, it will be for the politically competent bodies, for the Council, to take a decision. But perhaps the Council will want to see how its current arrangements work in practice before it addresses the need to go further. Again, I believe that within the institutional framework of the Union, which is bottom up and not top down, there may also be constitutional limits on what the EU could or could not do on the basis of the current treaty. But, frankly, it is for more eminent experts in this House than I certainly claim to be, to look at these legal questions.

Q232 ***Chairman:*** Mr de Vries, could I thank you very much for coming to give us your evidence and the answers to our many questions this evening. It has been an extremely helpful and very useful session for us and we have learned a great deal more about the work that you do. We wish you well for the future.
Mr de Vries: Thank you very much.

Q233 ***Chairman:*** We will of course send you our report when it is concluded. Once again, may I say thank you on behalf of all of us here.
Mr de Vries: Thank you very much.

WEDNESDAY 10 NOVEMBER 2004

Present	Avebury, L	Harris of Richmond, B (Chairman)
	Corbett of Castle Vale, L	Listowel, Earl of
	Dubs, L	Ullswater, V
	Gibson of Market Rasen, L	Wright of Richmond, L

Memorandum by the Information Commissioner

INTRODUCTION

1. I welcome the opportunity to submit evidence to the Sub-Committee. As Information Commissioner I have no objection, in principle, to the freer exchange of data between law enforcement authorities in the EU provided such exchange is a necessary and proportionate measure for the prevention and detection of terrorism or other criminal activity and there are appropriate safeguards for privacy. Similarly, I have no objection to the principle of equivalent access to data by national law enforcement authorities in the EU. I can see no reason why, for example, the French police investigating a murder in Paris should not, in principle, have access to the same information in the UK that the UK police would have if investigating a murder in London. The French police must, of course, be able to satisfy the same tests of necessity and proportionality that the UK police would have to satisfy and must be under an obligation to treat any information received with the same degree of respect.

2. It is essential that the privacy of personal information is not unduly compromised by moves to increase the exchange of or access to data. Safeguards are needed to protect the position of individuals. Principally these safeguards are delivered through data protection controls. The existence of such controls, that are broadly equivalent in each EU member state and relevant EU body, is a necessary counterbalance to greater data exchange and access. The question is whether sufficient controls are already in place or whether a new, common legal framework for data protection is needed to deliver them.

3. There is a parallel here with the First Pillar. In the First Pillar there is a Data Protection Directive (95/46/EC). It was introduced to facilitate the free flow of personal information within the single market. Article 1 of the Directive provides that member states shall neither restrict nor prohibit the free flow of personal data between member states on privacy grounds. In effect the principle of free exchange of data and equivalent access is already established in the First Pillar. It is though established on the basis that member states must implement the data protection controls in the Directive through their national laws and must provide redress for individuals where its provisions are breached. There is also a requirement for independent supervision. In the First Pillar it was considered necessary to use an EU legal instrument to ensure that broadly equivalent controls are in place throughout the EU as a counterbalance to the removal of cross border restrictions on the exchange of and access to personal information. In this context, it should be noted that although most member states had already ratified the Council of Europe Convention on Data Protection (Convention 108 of 28 January 1981) the provisions of this Convention were not considered to be sufficient to deliver the degree and consistency of protection deemed necessary.

CURRENT DATA PROTECTION ARRANGEMENTS

4. The question to be considered is whether the existing data protection controls in the Third Pillar provide sufficient protection in an era of increased information exchange and access. There is no equivalent of Directive 95/46/EC in the Third Pillar. My understanding is that most member states, although not obliged to, have extended their national laws implementing the Directive to law enforcement agencies. The other member states have specific data protection laws covering police files. In addition all member states have now ratified the Council of Europe Convention on Data Protection (Convention 108 of 28 January 1981). Account should also be taken of Recommendation No R(87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987 on the use of personal data in the police sector. Member states, to varying degrees, have incorporated the principles of this Recommendation into their national laws and practice but it is not a binding legal instrument.

10 November 2004

5. I am not in a position to comment in detail on the adequacy or otherwise of data protection laws in other EU member states. There is certainly no evidence available to me to suggest that data protection controls applying to law enforcement authorities are inadequate elsewhere. There may, nevertheless, be significant differences between member states. It is also the case that the legal framework of the EU does not currently underpin these controls nor does it ensure equivalence of protection across the EU in the same way that is achieved by Directive 95/46/EC in the First Pillar. This is a potential weakness. Differences in the law and practice across member states could become more apparent and act to the detriment of individuals as cross border access to and exchange of information increase. This in turn creates a risk that data protection could become an obstacle to increased cross border co-operation in the Third Pillar. If the divergence of laws increases in the future so will this risk. There must therefore be some merit in the proposal for a common EU data protection legal framework for the Third Pillar.

6. The position of EU bodies and systems such as Europol, Eurojust, the Schengen Information System and the Customs Information System need to be considered. Each of these has its own data protection controls incorporated into the legal instruments under which it is established. To varying extents these controls are based on Convention 108 and Recommendation No. R (87) 15 of the Committee of Ministers of the Council of Europe. These bodies and systems also each have their own independent data protection supervisory body on which my office and the data protection authorities in the other EU member states are represented.

7. It is hard to conclude that the arrangements for EU bodies and systems fail to provide adequate protection for personal data. The problem is more that the proliferation of different legal instruments and supervisory arrangements governing data protection is confusing, inflexible and disproportionately consuming of the limited resources available to data protection authorities including my own. To the extent that a common EU data protection legal framework for the Third Pillar would address these deficiencies without weakening the existing standards of data protection it would be welcome.

A Data Protection Legal Framework for the Third Pillar

8. For the reasons set out above I am inclined to support the case for a common EU data protection legal framework for the Third Pillar. My concern is that it should not undermine existing data protection provisions. It is important that any legal framework addresses the specific issues that arise in the Third Pillar and goes beyond simply restating basic principles of data protection. The framework should draw as much, if not more, from Council of Europe Recommendation R(87) 15, relevant legal instruments in member states and original thinking as it should from the existing EU data protection instruments in the First Pillar.

9. The relationship between any new legal framework and the existing rules applicable to relevant EU bodies and systems will need to be considered. Clearly, these bodies and systems should come within the ambit of a new framework but the existing data protection controls, which in some cases are very specific to the body or system concerned must not be lost. A review of these may be desirable but under any new framework some provision for data protection controls that are specific to individual EU bodies and systems and that have legal force needs to be retained.

10. There also needs to be a mechanism through which there can be a data protection input to new developments in the Third Pillar of the EU. In the First Pillar there is both a working party of data protection commissioners (the Article 29 Working Party) and the European Data Protection Supervisor who have a role in advising the Commission. In the Third Pillar there are existing supervisory bodies but they have a limited remit. There is currently no formal means through which there can be an independent data protection input to developing initiatives.

Transfer of Personal Data to Third Countries/Bodies

11. Any new legal framework for data protection in the Third Pillar would need to address the question of international transfers of personal data. The principle, established in the First Pillar and in the Europol Convention, that transfers should only be made to third countries and bodies that provide an adequate level of data protection is a sound one. There must of course be scope for exceptions to take account of transfers, even to countries that do not provide adequate protection, where there is an overriding public interest. In the context of wider access to and sharing of data there is a real risk that controls on the international transfer of personal data operating in an EU member state or body could be circumvented if there are no common standards for transfer. For example, it would be unacceptable if UK restrictions on the transfer of data from the UK police to the police in country X could be avoided by the police in another EU member state, where

there are no such restrictions, accessing the UK data and then making the transfer to country X themselves. There must also be practical benefits in a system whereby determinations of adequacy can, but do not necessarily have to be made centrally. If such central decisions could then be relied on by EU member states and bodies the need for each member state and body to separately make its own assessment would be avoided and a degree of consistency could be ensured.

Richard Thomas

15 September 2004

Examination of Witnesses

Witnesses: MR RICHARD THOMAS, Information Commissioner and MR DAVID SMITH, Assistant Information Commissioner, examined.

Q234 ***Chairman:*** Good morning Mr Thomas and Mr Smith. For the record, if I just inform everyone that Mr Thomas is the Information Commissioner and he is accompanied by Assistant Commissioner David Smith. You are both very welcome to the inquiry to give evidence. Thank you very much indeed for the evidence you have already submitted to us. We will have a number of questions on that but we have all read it and we are most grateful to you for sending it to us. Again, for the benefit of people who might be wanting to understand what we are doing, the subject of the inquiry is an examination of a number of proposals designed to strengthen EU counter-terrorism activities, particularly through much more extensive data exchange. These proposals raise important issues, not least in connection with data protection. Therefore it is our wish to obtain the views of the Information Commissioner. I think you have been sent a copy of our interests relevant to the inquiry so that you know what the various interests of members might be. I wonder, Mr Thomas, if you would like to make an opening statement to us and then we will launch into questions.

Mr Thomas: Thank you very for that welcome and for the invitation to address this Committee. We very much welcome the opportunity to assist you in this important inquiry. So that you understand, I am the Information Commissioner responsible for both the data protection legislation in this country and also freedom of information legislation. David Smith is the Assistant Commissioner responsible for police and law enforcement matters. He also has extensive experience with the joint supervisory authorities for Europol, Eurojust, Schengen and the Customs Information System. We very much welcome the subject matter of this inquiry. As you have mentioned, we submitted a written memorandum to you; we are happy to take questions on that. We are also familiar with—and, indeed, endorse—the Opinion which you received from the four joint supervisory authorities which has been sent in separately. I understand you met some of the members of that grouping in Brussels last week.

Q235 ***Chairman:*** Yes, we did.

Mr Thomas: The Treaty of Amsterdam objective is set in very important terms of establishing an area of freedom, security and justice and giving priority status to the fight against terrorism. I think that has to be set against an environment where in policing matters we are seeing a trend for far more information to be collected by law enforcement authorities and to be exchanged. Perhaps one is also seeing a trend going beyond those who are just suspects, as it were, where there is an active matter being investigated—but a trend towards greater profiling of individuals. I think that this does raise very important questions about the inter-relationships between data protection and the fight against terrorism and other serious crime. These questions arise at the domestic, the European and the international level. I think perhaps we have two key messages we would like this Committee to take on board. The first is that the more that there are to be exchanges of information, the more it is important for the information to be necessary and proportionate for the intended purposes, whether that is a fight against terrorism (prevention or detection of terrorism) or serious crime. In other words, data protection safeguards are a very important counterbalance to the trend towards greater exchanges of information. I think that this does, to a certain extent, make these exchanges more acceptable to the public at large. The public, I think, from our experience and from surveys we have conducted do take these matters seriously; they understand why the authorities need to have an exchange of information but they do want safeguards in place. Safeguards are needed to protect individuals, to ensure that their personal privacy is not compromised unduly by moves to exchange information or increasing access to information. The second key message—I am sure it will come out further in questions and answers—is the need, in our view, for a new common legal framework for policing and related matters across the European Union. Obviously that is one the proposals now coming from both the Commission and from the Council which I anticipate we will discuss in more detail. In general

terms, subject to some provisos, we very much welcome the trend towards a common legal framework.

Q236 ***Chairman:*** Thank you very much indeed. That is a very helpful opening statement. My first question to you, which you have begun to give a framework of answer to—you talk about having a common legal framework and safeguards—but I wonder if you would like to expand a little bit more on the role of the Commissioner.in relation to the data protection implications of EU proposals.

Mr Thomas: I am a creature of statute; my office was created by the Data Protection Act and modified by the Freedom of Information Act. I am an independent regulator. In European jargon I am an independent supervisor. I think it is very important to stress this point. I am not part of the Government; I am independently appointed and, indeed, accountable directly to Parliament. My responsibilities are primarily UK focussed. I have a range of responsibilities in relation to data protection matters in the United Kingdom in terms of regulating data controllers; in terms of promoting good practice; in terms of resolving disputes and so on. The 1998 Act does have a section—section 54—which deals with international cooperation. For example, through that I participate in what is known as the Article 29 Working Party, which brings together the independent supervisory authorities across the European Union for the purposes of the existing data protection directive. Of course, that is a single market measure—that is the directive of 1995—and that does not, as a directive, extend into policing matters. The 1998 Act domestically does cover policing matters and that was a decision taken when the legislation was passed through. My role at the European level in policing matters is really quite limited. We do participate in the joint supervisory board or authority, as I have mentioned, for the four institutions: Europol, Eurojust, the Schengen Information System and the Customs Information System. What we do not have is any formal role at all in relation to the proposals which are now being put forward. They are proposals which are coming forward for a wider approach to exchange of information and the data protection aspects of that. Informally we are asked for views, for example by the Home Office and we are delighted to be addressing you here this morning. However, as an independent national body—and indeed in collective terms with our counterparts across Europe—we have no formal role.

Q237 ***Chairman:*** Is that something you would wish to have?

Mr Thomas: Indeed. One of the matters which my colleagues and I across Europe have discussed is the creation of some sort of counterpart to the Article 29 Working Party, a forum where we can come together in a more formal environment and can review the various proposals coming forward and express our views on those matters. If I can use a metaphor, it is that of building new buildings and I think we would like to be involved at the architectural stage, not just once the building is up and in place. We meet informally on a number of occasions, most recently in Poland in September in the city of Wroclaw. A resolution was adopted then by all the European independent supervisors calling for the establishment of a new forum, a Third Pillar forum, for us to have a more formal role in responding to initiatives relating to personal data at this level. I think the Committee has seen a copy of the resolution and we were part of the process of producing that resolution.

Q238 ***Chairman:*** You had the very strong understanding that all information commissioners felt exactly the same way?

Mr Thomas: I think there is no doubt about that. David may wish to elaborate. I have only been on the scene for just under two years, but David has been doing this sort of work for ten years or so and has very good linkages with our counterparts on policing matters. I think it is a universal view.

Mr Smith: It is a universal view. I think if there are developments in the law enforcement field in the UK for example on information sharing, I hesitate to say always—but almost always—the Government will consult us and we will have a close dialogue. We do not always reach agreement but we always have a useful discussion. There is no equivalent mechanism for developing initiatives in the EU where that independent data protection input can be put into the developing thinking. That really is what all the data protection commissioners would like to see; some sort of committee or body with a relationship where there can be communication between the Council and the data protection community.

Q239 ***Chairman:*** Could I ask if you have had any sort of feedback about your concerns? If this is universal, someone somewhere ought to be taking great note of what you are saying.

Mr Smith: We may be coming on to something we will touch on later. We know that work is going on in the Council to develop a framework decision on data protection. Whether it will cover this or not we do not know. I would very much hope it would do, but we have not seen any drafts of that, we just know that the work is on-going.

Chairman: I am sure we will develop that later on. Lord Dubs?

Q240 ***Lord Dubs:*** Just in case I misunderstood, when you were talking about a common legal framework, Mr Thomas, was that something that you envisaged encompassing the point that has just been made or was that a separate thing?
Mr Thomas: I think we are aware unofficially that proposals are being worked up, but we still have to pick these things up almost in the corridors rather than through any formal mechanism. Given that we are a very busy organisation we do not always have the time, effort and resources to bring this information together. We are aware informally of the various issues but we do not have the full detail in chapter and verse. However, we would like to be more formally involved; we would like to be consulted. I am not sure whether that answers your question fully but it is exactly the sort of ground that David was mentioning.

Q241 ***Lord Wright of Richmond:*** Is your non-involvement in any way related to the British Government's position vis-à-vis Schengen?
Mr Thomas: I do not think directly at all, no. David you sit on the Schengen Information System as an observer, do you not?
Mr Smith: That is right. On the Schengen joint supervisory authority we sit and we have observer status at the moment. When the UK joins the Information System next year we will be elevated to full members. However, in practice we can participate in the same way that everybody else does.

Q242 ***Chairman:*** One final question on the introductory remarks you made, you talked about surveys that you had done with the public or the public's view about data protection matters. Where could we see these surveys?
Mr Thomas: For many years now we have conducted a tracking survey asking the general public for their experiences and attitudes towards both data protection, and now freedom of information, matters. We ask a series of questions which we have modified slightly over the years. They are published on our website every year. They are produced in a rather more graphic form this year; they were put there about two or three months ago. We could send them to the clerk if you would like to have the most recent results. They are very general. They cover a wide range of opinion and experience in relation to data protection matters. The general point I was seeking to make is that the public do clearly take privacy and the handling of their personal information very seriously. It is ranked, alongside other public concerns, really quite highly.

Q243 ***Lord Avebury:*** I was just wondering whether there was any example you could give us of an occasion when the Commission, the Council or the European Parliament have failed to ask your advice under the informal arrangements that exist to an extent where directives have been produced without proper consultation.
Mr Thomas: I cannot think of a specific example during my term of office apart perhaps from the subject matter under discussion this morning. We read that proposals are under development. I have to be frank with you, I see the papers coming from the Commission, I saw very recently the Hague Programme coming from the Council; I am not sure that I entirely understand the relationship between these and who is drafting them and how they are being put together. Certainly we have had no formal consultation nor, to my knowledge, have my colleagues across Europe.
Mr Smith: If I could just add, the consultation we have tends to be hit and miss in some ways. In the documents that you have been looking at we have been asked by the EU Scrutiny Committee for comments on the proposal on the exchange of information from the Kingdom of Sweden, but we have not been asked by anybody other than yourselves for any comments on the Commission proposal on enhancing access to information. We do have some things to say on that. One other area where we have had some concerns is the development of the new version of the Schengen Information System, SIS II, where the joint supervisory body has given an opinion on that but at a fairly late stage. Our concern has been that in developing any new system the starting point should be, what is the purpose? We still have not seen a clear definition of what the purpose of SIS II is but until you know what the purpose of the system is it is hard to make a proper data protection judgment. Those are just a couple of examples.

Q244 ***Chairman:*** When our report is published I am sure your evidence will be published with it and your views expressed clearly through that. Thank you very much indeed. Could I move on then to my second question? In your evidence, Mr Thomas, you say, "I have no objection in principle to the freer exchange of data between law enforcement authorities in the EU provided such exchanges—and again you reiterate—are a necessary and proportionate measure for the prevention and detection of terrorism or other criminal activity and there are appropriate safeguards for privacy." Could I ask, who is going to judge whether that criterion is met and what sort of mechanism would be put in place to ensure that it is?
Mr Thomas: As I indicated in my opening statement, those two words "necessary" and "proportionate" and the phrase "safeguarding privacy" are fundamental to what data protection is all about. The way it works—and the way I would anticipate it working in the future—it would be for the law

enforcement agency themselves in the first instance to make judgments about necessity and proportionality. The way the legislation works is that people are required to think long and hard about what they are doing with personal information and to ensure that they can justify what they are doing. They are entitled to process personal information in accordance with data protection requirements. They must not go beyond that which they can justify. That is the way it has worked in this country under the 1998 Act and, indeed, the 1984 Act before that. The law enforcement authorities—the police and the other authorities in this country—have to ensure that their access to information, their use of personal information is necessary and proportionate. They, themselves, must be able to justify their actions. They may be challenged on that and that is where the role of the independent supervisor comes in. Part of my role is to challenge on some occasions whether they are getting it right. I would hope that a formal challenge would be fairly exceptional because I see the role of the regulator as much in terms of giving advice, promoting good practice and helping organisations get it right in the first place. That is why, for example, we have a code of practice which has been developed over the years, which is the code of the Association of Chief Police Officers relating to the processing of personal information within the United Kingdom. I do not think it is appropriate to go into too much detail this morning but there was obviously controversy over that code with the Soham murders and the Humberside police, but I think it was well established in that particular case that it was not the code or the data protection legislation that was causing the problems; ironically it was probably the police having too much information and losing the information within their computer system. That is a rather good example of the importance of good information handling. I digress a bit from your question. The answer to your question is that primarily it is the data controller, the person holding the information, but subject to challenge by the independent supervisor. Of course, if a challenge is not accepted there are mechanisms through tribunals and ultimately through the courts to make rulings in particular matters.

Q245 ***Chairman:*** Has there ever been a formal challenge?

Mr Thomas: In the United Kingdom I have actually served notices in the last two or three months on three police authorities where I believe they are holding information for far longer than is necessary. These are all cases where individuals committed fairly minor crimes in their late teens—in one case aged fourteen—where people are now approaching late middle age. Those matters are still on their record and the police believe they should stay on their record until those people are one hundred years old. I am not prepared to accept that approach. The police take a different view and they have appealed my formal enforcement notice; the matter will now be heard by the Information Tribunal, which is the proper place for these issues to be resolved. So yes, where appropriate, we will take enforcement action.

Q246 ***Lord Wright of Richmond:*** I am sorry, I do not really want to pursue this particular point, but surely the stories in the press today of a possible murderer of Miss Nickell does actually rather support the police case for holding records longer than shorter.

Mr Thomas: Perhaps David will say a little bit more about this in a moment, but I think there may be a case for basic information to be held and perhaps DNA material to be held in particular cases. I understand the point you are making, but whether you need to have information about offences committed many, many years ago where people have completely rehabilitated themselves and are trying to lead decent honourable lives and are finding this increasingly difficult now in a climate where past convictions are being sought out through the Criminal Records Bureau and people are being disqualified from jobs. I think one needs to draw a balance there. It is a difficult issue, I fully recognise that. I do understand the point you are making, Lord Wright, but I still would argue the case for a balance.

Mr Smith: I think that we are satisfied that Parliament has struck a balance in deciding that DNA and fingerprint information can be kept for life when it has been taken lawfully. We very strongly link that to the need to continue to be able to identify people which is at the centre of the case which is in the papers today. Our concern is that the police are seeing this as a licence to keep all the information. If someone was arrested but never charged fifty years ago, they still want to keep the details of why they were arrested. We have no problem with the identifiers, it is the other information. I think perhaps also the case in the papers today, although I would not want to make too much of it, illustrates in other ways perhaps some of our concerns because it appears to be a case where the police became convinced that someone was guilty and tried to build up a case and indeed went too far in building up that case. There is always a risk as we get more and more information that you see patterns; patterns can be merely coincidences and you read too much into the information and the information can be unreliable as well. We would not want the police ever to lose sight of the need for proper judgment and proportionality and the correct approach.

Mr Thomas: Could I make one further point in answer to your previous questions? I talked about regulation using enforcement powers; I talked about advice and support and promoting good practice.

What I did not mention was one feature which we lack in this country which is an audit power, a power to inspect and audit what is going on. Most of our European counterparts do have the power to audit. We can only do this with the consent of the data controller and that does rather handicap what we can do. To have to say to someone holding personal information, "May we please come and see what you are doing and only do it with your consent?" is quite a handicap. We do have a power of audit in relation to Europol and Schengen so we can go knocking on the door of NCIS, and David has done this a couple of times.

Q247 ***Chairman:*** That is what I understood.
Mr Thomas: We can do that under the Europol Convention and the Schengen Information System but more generally we do not have that power. That is something we have raised with the Department for Constitutional Affairs; the European Commission has already raised some concerns about this point in relation to the principal directive and it is a power which we very much believe we ought to have. I think it is relevant to matters which this Committee is reviewing.
Chairman: Thank you for raising that; it is a very important piece of information. Lord Avebury?

Q248 ***Lord Avebury:*** My question follows neatly on the answer you have just given and on the previous answer by Mr Smith. I was wondering how on earth do you decide on proportionality when you are dealing with the profiling of individuals and not with actual convictions. Any member of the public can understand—as Lord Wright has pointed out—why it may be necessary to retain information about convictions for a very long time and particularly the evidence of DNA and so on. However, when the police have reasons, as they see it, for example to suspect that someone is involved in terrorist activities and they build up the profiles—as you mentioned in your introductory remarks—there may be an enormous number of false positives. What I am wondering is that if you do not have any power of audit, as you have just said, how on earth do you judge the proportionality of the police putting an enormous amount of effort into collecting data which may be completely irrelevant to the problem of terrorism?
Mr Thomas: I think you have raised some really fundamental issues and I do not believe there are easy answers in this area. We all wish and hope that where there is a strong indication of terrorist activity then the authorities are on to that and are able to deal with it. However, the formal answer I have to give is that in determining proportionality the police themselves have to justify what they are doing. We have to be satisfied that a case has been made out, but I think it is a discipline—there are no black and white answers—upon the police to make sure that they are observing these requirements. I think implicit in your question is a recognition that sometimes too much information can be collected. I think there is some indication of that from the American inquiry into the 9/11 tragedy that the enforcement authorities there perhaps had some information about the terrorists in question but it was buried in a mass of other information. Perhaps that is what happened, in effect, with the Soham murders in this country. One of my colleagues put it recently that, if you are looking for a needle in a haystack, do you make the haystack any bigger? One has to make sure that the information being collected is pertinent to the matter in question. I do recognise that the police and the security authorities do have a massively difficult job and getting the balance right is not easy.

Q249 ***Lord Dubs:*** You referred a little bit earlier on in answer to a question about the case of the young man and the police keeping records for a very long time. If you have no audit powers, how do you know whether the police are not doing this on a very wide scale and how did you find out about that one?
Mr Thomas: That is an extremely good point you are making because a lot of activity is hidden away from public view. The public at large are perhaps not aware of what is going on. We come across these cases where people make complaints to us against the police authorities. In one of the cases I mentioned, the woman—I think she is now 48 years old—had a dispute with her next door neighbour. He was a police officer who discovered by accessing the police national computer—quite improperly, in my view—that she had committed an offence when she was fourteen years old and brought this to her attention. She, quite rightly, complained to us; we have served an enforcement notice. However, I have to recognise straightaway from what you are saying, Lord Dubs, that these are exceptional cases where people come to us by way of complaint. As more and more people now see their entry on the Criminal Records Bureau—because people need their certificate for employment purposes—more and more people are now seeing what is held on them and are perhaps getting more concerned about this and are coming to us as a result. At the moment, without the audit power, we have to rely almost exclusively upon complaints brought to us.

Q250 ***Chairman:*** I wonder if I could just clarify a point that is slightly troubling me as a former chair of a police authority. You keep referring to police authorities having responsibility for this and indeed police authorities have to pay out when the police force gets it wrong, but it is an operational point, it is

the police force who deal with the actual incidents and do the recording.
Mr Thomas: I stand entirely corrected. My expert, David Smith, has put me right as you have, indeed. I do apologise; I should have used the phrase "police force" throughout.

Q251 ***Lord Corbett of Castle Vale:*** On this issue about police forces, they hold that information generally on the police national computer although they will also have their own force database. You are having to act on the assumption that that information is accurate. We do know from experience that a lot of information on the PNC is inaccurate both ways; there is no conviction when they say there is and vice versa.
Mr Thomas: The Bichard Inquiry—the inquiry headed by Sir Michael Bichard—into the events at Soham, has, I think, brought very, very forcibly to the surface really quite serious concerns about the nature of the police national computer, the quality of the data and so on. Perhaps David will say a bit more, but we do come across cases of inaccurate information held there.
Mr Smith: We would make a general case for a wider audit power for our office, but I think today it is really a case of an audit power for the police that we are concerned with. As Mr Thomas said, it is so important to individuals and so much of it is hidden. The examples we see are where a window is open because there are things like the Criminal Records Bureau disclosure process which gives people an insight into the information which is kept. We do have a power in relation to Europol and Schengen, that is in relation to existing mechanisms which have been set up for the exchange of data within the European Union. If there is to be an extension I think it follows that we ought to have an audit power to look at what is going on there and ensure that it complies with these proportionality requirements. There may be just one other point to add on the proportionality requirement. I hesitate to talk about more formalisation because I think when we gave evidence to this Committee before, we were critical of the over-formalisation of some of the data protection procedures in the European Union, particularly in relation to Europol. Here where decisions have to be made on whether access is necessary and proportionate there could though usefully be some guidance on how those decisions are made, some requirement to record them, something that, if you like, we can audit against. Given the capability of computer systems these days it ought to be fairly easy to record these sorts of things as part of an audit trail on a computer system which we can then centrally check on.

Chairman: Thank you very much, Mr Smith. I ought to remind members who were not part of the sub-committee at that time that you are an old friend of the Committee having given evidence before to our Europol Inquiry.

Q252 ***Lord Wright of Richmond:*** I apologise for prolonging this particular questioning, but you said that at least some of your European opposite numbers have an audit power which you would like to have and which you do not have. Is it your experience that those countries which have an audit power for the information commissioner have actually been able to uncover and remove the imperfections that you think exist in the police procedures in this country?
Mr Smith: To give a categorical "yes" would be going too far. Our understanding is that all the authorities have an audit power but I am reluctant to state that as a fact, but it is nearly all of them if it is not all of them. There is no doubt that they use it in relation to the police. I could not tell you just what they have uncovered and what actions they have taken.

Q253 ***Viscount Ullswater:*** I want to ask one question on proportionality. Is there a common standard of proportionality amongst 25 European Union states?
Mr Thomas: No, there is not. I am not sure that there could be because I think proportionality always needs to be addressed essentially on a case by case basis. One looks at the circumstances of a particular matter so, although there is not a single standard, what there is is an ever-increasing understanding of the approach to be taken. I would say it is almost a theology; it is a set of principles to be applied, if you like putting the burden of proof on the data controller to demonstrate how, and the extent to which, their actions are proportionate and then to be able to justify those. On occasions they are challenged on a case by case basis but in accordance with principles. There is no single standard and I very much doubt that there could be.
Chairman: My Lords, the number of questions we have asked is a measure of the great interest that we have in this matter and the very helpful remarks that we are having from both Mr Thomas and Mr Smith, but we now must move on. Could I ask Lady Gibson to continue?

Q254 ***Baroness Gibson of Market Rasen:*** Thank you. In your paper it comes through very strongly that you believe in strong safeguards for personal data. I wonder if you are aware of any cases of serious misuse of personal data in the law enforcement field.
Mr Thomas: Our experience is largely UK based, as you will appreciate. I very much hesitate to say that there is serious misuse in the sense of deliberate abuse. We have come across cases where individual

police officers have misbehaved in relation to information held on the police national computer and elsewhere, sometimes using it for their personal purposes, sometimes even selling the information. These are all criminal offences under Section 55 of the Data Protection Act and we have taken action in some cases and we have threatened in other cases. I think the problems are not deliberate abuse by police forces in the sense you are suggesting, but rather concerns—as we started discussing this morning—over accuracy (as Lord Corbett has already mentioned) over retention periods, and over the lack of safeguards being rigorously applied. We do have some concerns that if inaccurate information were to be exported from this country elsewhere into Europe, or received from Europe into this country, then problems could arise. We have had some examples in recent years of the sorts of problems which can arise. The Committee may recall the case of Mr Kenneth Bond. He was the Bristol Rotarian, a very respectable man in his late sixties or early seventies, who was arrested and held in South Africa on an FBI warrant. He spent nearly two weeks in prison in Durban and it eventually turned out that the FBI thought that he was one of their most wanted criminals. That was a classic example of identity theft where the real gangster had taken over the identity of Mr Bond in Bristol. That is an example of very serious detriment which can occur to individuals. On perhaps a less serious scale, there have been examples of football supporters travelling elsewhere in the world where information has not been entirely accurate about their background or there have been misunderstandings. David, I think you have some knowledge of the World Cup in 1994.

Mr Smith: Yes, there are two cases in particular that we are aware of. One was to do with the 1994 World Cup, which was held in the United States. Information was sent over there about potential hooligans visiting the World Cup. An individual was, some years later, refused entry when they went to the United States because this information had gone onto the immigration service stop list. My understanding is that the information had come from NCIS and NCIS never suspected for one minute that the information would be kept and used for these other purposes. That is a classic example. There was also one of some Welsh football fans who went to Belgium. When they were asked to produce their identity cards in Belgium and had not got them or refused to produce identification they were essentially sent out of the country. This information then went back to the UK and they ended up on the football hooligan database here. They happened to be visiting a football tournament but the incident was nothing to do with football. The potential for muddle, confusion and inaccuracy is so much greater when you move across borders.

Q255 ***Baroness Gibson of Market Rasen:*** You are saying that it is more muddle than deliberate in those circumstances.

Mr Smith: Yes.

Q256 ***Baroness Gibson of Market Rasen:*** You mentioned briefly the Hague Programme. Apparently the Commission see the principle of equivalent access to police data by national law enforcement authorities as the way forward and the Hague Programme refers to the principle of availability. Can you see any problems in these proposals in relation to data protection?

Mr Thomas: As I mentioned earlier, Baroness Gibson, I do not fully understand the relationship between the proposals coming from the Commission and the very recent programme coming from the Council so I put in that caveat to start with. I think I have to repeat what I said at the outset and in my paper, that I have no objection in principle to either equivalent or available access—whatever the distinction between those two concepts is—provided that the information exchanged is necessary and proportionate and that the safeguards are put in place so that there is due respect for data protection principles and the other safeguards. I think that there may be some specific problems with the proposals although I suspect that as one works towards elaborating those one could address these problems and still achieve the objective. One needs to elaborate exactly what are going to be the data protection safeguards in this area. I was quite encouraged, reading the Hague Programme, to at least see a marker put down there; and indeed, to be fair, in the Commission proposals they have talked about bringing forward measures. In the Hague Programme the document at paragraph 2.1 refers in particular to information being exchanged where—and I quote—"a law enforcement officer in one member state needs—*I emphasise 'needs'*—the information in order to perform his duties". So at least that concept is there. It goes on to talk about taking into account the requirement for the on-going investigations in the relevant states. Again I think that introduces the concept of proportionality. The document goes on to talk about the exchange only taking place in order that legal tasks may be performed and the integrity of the data should be guaranteed, and so on. Then it goes on more explicitly to refer to "supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured" and that "individuals must be protected from abuse of data and have the right to seek correction of incorrect data". I do not know who has drafted this. As I mentioned earlier, we have not been consulted on it. It is only through the good efforts of your Committee that this was drawn to our attention in the last week

or so, and I emphasise that point. Having said that, somebody has recognised the point I made at the outset. If there is to be more exchange then it must be counter-balanced by appropriate data protection safeguards. At least this document does put down the marker. This will now need to be elaborated to address the sorts of risk which might otherwise arise. You did ask about what sort of problems we might see with these concepts and David might like to elaborate. We can speculate that there could be some problems because of different standards in different countries across Europe.

Mr Smith: I think a lot depends on what you mean by "equivalent access". We are not very keen on the term "equivalent access" because if access—and I am not saying it is—were slap-dash in the UK why should the rest of Europe be entitled to a slap-dash regime. If access is tightly controlled and proportionate and necessary as we have said, then the principle that any police officer anywhere in Europe who can make a justified case ought to be able to get access is sound. That, in many ways, is what the European Union is all about. I would think that that is our concern. I mentioned before the question of interpretation of information. If there is equivalent access, is it meaningful to a Spanish police officer? We did have a case where a drugs intelligence report was sent to Spain and then was quoted in a Spanish court as a conviction. That is not deliberate misuse, but misinterpretation of information. Things like offences which vary from country to country—particularly in very sensitive areas like offences connected with homosexual acts and abortion, things which are an offence in one country but not in another country—do you give access or not? There are some very difficult issues to be sorted out. It is worth raising here an area where we have some doubts. There are mechanisms for exchanging information within Europe at the moment. There is Europol, there is the Schengen System, there are informal arrangements between police forces; nothing stops the French police exchanging data with the UK police. When we go and do our inspections of Europol we are told all the time—particularly by Europol—if only people would send us more data and if only they would update the data they send. The EU proposals are very much concerned with more legal instruments which may be helpful but we do wonder whether lack of legal instruments is the nub of the problem or whether it is more to do with the policing culture of protecting sources and not trusting others with our information. There must be at least as much of that to it as a lack of a legal framework.

Chairman: That is very helpful, thank you. You have raised some very interesting points. Lord Corbett?

Q257 ***Lord Corbett of Castle Vale:*** The other aspect of this which really lies behind a large part of the inquiry we are doing is as a result of the 9/11 Commission Report in the States. In the summary here they mention the FBI having no effective mechanism for capturing and sharing its institutional knowledge. Then it makes the point—and this is really the point we are on—that the perceived legal barriers to the sharing of information known by staff, widely known as the wall, which blocks the sharing of information both within and between the agencies. I think that is very much on the point here because the Commission has emphasised the need to enhance the inter-operability of EU databases. Do you think this is likely to give rise to new data protection problems?

Mr Thomas: On the general point you are making I think within the UK, and maybe more widely across Europe, there are still some misunderstandings about the extent to which data can be shared and I think one of my tasks is to make sure that the misunderstandings are dispelled. I mentioned earlier promoting good practice and providing advice and I accept that we perhaps need to address some of the misconceptions and misunderstandings. That is the general point I want to make. In terms of the inter-operability of the various databases, we are not quite sure what exactly is being proposed, that is why I am afraid we can only respond in general terms at this stage. I do not have any difficulty with it if it were going to be an exchange of information which is legitimate and people understand how and why it is being done. I do not have any objection to that being done through two or more databases talking to each other. That is a familiar issue for us. What we would say, when there is to be an exchange of information, it must be done in accordance with explicit data protection requirements. We are looking for a framework to ensure that that does happen in practice.

Q258 ***Lord Corbett of Castle Vale:*** One can see, I suppose, in the case of serious organised crime and terrorism the need is easier to demonstrate. Is it your understanding that it is this kind of practical sharing where it has been proved to be necessary and proportionate that this is directed at?

Mr Thomas: That is my general understanding, Lord Corbett, but I do not pretend to have a detailed understanding. I think to be honest those are questions which are perhaps better addressed to the law enforcement authorities themselves or to the Commission or to those making these proposals. I am not really able to answer that with authority.

Q259 ***Lord Corbett of Castle Vale:*** The Commission's most recent proposals envisage access by law enforcement authorities to the databases of financial institutions. Do you have specific concerns about that?

Mr Thomas: Yes, I do. I am not aware of the detail of these proposals. I take the general point that there are undoubtedly important links between terrorism and the preventing of terrorism and I understand the need. The money laundering regime is clearly directed at those sorts of problems. I am aware of the general issue but I think one needs a great deal of caution if anyone is contemplating direct access by law enforcement authorities to, quote, "the databases of financial institutions". It is one thing for a police or a security service to get proper authorisation to inspect the bank details of a particular individual who is under suspicion; where that is done properly there are no problems at all and I have no difficulty with that. However, if people are contemplating regular and routine access—fishing or trawling—to the databases within financial institutions, then I think that does raise very major issues: issues of banking confidentiality, issues of privacy. It goes to the heart of Article 8 of the European Convention on Human Rights which safeguards privacy. I think we need to ask, where is the pressing social need to justify such a significant intrusion into the financial affairs of, ultimately, the entire population? I think there would be very considerable public concern if that were ever to become a routine matter. My position would be, as an absolute minimum, the law enforcement authorities need to justify access on a case by case basis and should have some sort of judicial or equivalent authorisation before they actually access that sort of database.

Q260 ***Lord Wright of Richmond:*** Mr Thomas, your written evidence expressed the need for a common data protection legal framework for the Third Pillar but you say it should address the specific issues that arise in the Third Pillar. What are those special issues? It is perhaps a naïve question, but would it not be possible simply to apply the First Pillar directive to the Third Pillar? Why is the Council of Europe Convention not adequate? What are the additional issues or principles that you want see addressed?
Mr Thomas: Thank you, Lord Wright; there are a lot of questions there and I will do my best to give you a comprehensive answer. I will answer your second question first, which relates to the First Pillar Directive, that is Directive 95/46/EC. I think that provides the background before moving on to your first and third questions. That Directive is the foundation for data protection law in this country. I think it is sometimes forgotten that it was put in place to facilitate the free flow of personal information within a single market. It is all about the very thing we are discussing today—exchanging information—but within the context of a single market. The principles—and we have been talking about them this morning—are broadly familiar, broadly acceptable, as is the principle of independence of supervision. There is no equivalent for the Third Pillar; there is nothing equivalent for the exchange of non-single market information, law enforcement information and so on. I think there is a strong case for something because, as more and more information is exchanged, I see two major risks in the absence of such an instrument. The first risk is that, as greater divergences emerge, there will be obstacles to the free flow of information. Those who are interested in getting more exchange I think will find more and more problems and obstacles as the divergences become apparent. Also, alongside that, there is a greater risk of detriment to individuals if information is being exchanged without a proper framework. I think I would say that the specific issues which you asked me about really arise out of the nature of policing and law enforcement. There are going to be issues relating to retention of information: how long should it be kept for? There are going to be issues about defining and limiting what are law enforcement purposes. There are going to be issues about information which is obtained under coercive powers. There are going to be issues about the reliability and the handling of information when it comes from a variety of sources of different reliability. There may be more specific issues in relation to information relating to racial matters, to religion and sexual behaviour and so on. I think these are all of a different species, if you like, to single market information which is essentially largely—although not entirely—commercial information being exchanged. The examples I have given, I think, demonstrate the differences and I think something is required which is specific, which is tailor made, for the rules which are required for the police and intelligence authorities to exchange information. If I were to be a little more provocative I would say that the existing Directive has its own problems and I would not want to see those transplanted and just applied to the policing area; I would rather make a bit of a fresh start. The existing Directive I find to be a rather uncomfortable mix of some very general matters and some very detailed specific bureaucratic measures and I think it is widely seen as not a particularly admired Directive. I think simply to transplant that lock, stock and barrel into this area would be a mistake; I would rather start with a clean sheet and address the specific issues thrown up by policing matters.

Q261 ***Lord Wright of Richmond:*** How about the Council of Europe Convention?
Mr Thomas: The Council of Europe Convention, if you like, is the sort of starting point for the directive itself; the directive bears a relationship to the Convention. The Convention is expressed in fairly

general terms. There is a document which I think the Committee will be familiar with, Recommendation 15 of 1987, which was from the Council of Europe. I think it is a Recommendation which flows from the Council of Europe Convention. That does explicitly address policing matters. That is a Recommendation and has no legal binding force but in this country the Government has taken it quite seriously and the 1998 Act does go quite a long way to meet the recommendations for policing matters set out in that document. I do not think that document should simply be made legally binding across Europe—that would not be the answer—but I do think that goes 75 or 80 per cent of the way towards the substance of what we would be looking for in a common legal framework for Third Pillar matters. I do see Recommendation (87) 15 as a very good starting point, but not the end of the story.

Q262 ***Lord Wright of Richmond:*** To what extent does either the Council of Europe Convention or a draft legal framework for the Third Pillar take into account the problem that Mr Smith has referred to, ie the differences between Member States in the position on, for instance, homosexuality or drugs?
Mr Smith: You are perhaps taking it a little bit further than we have thought through. There is no doubt that it would need to take that into account and recognise that information which is about offences which are not offences in one country but are in another ought to be restricted. You may be getting to the purpose definition in certain areas. There need to be principles to do with the exchange of information which are set out—but those should only apply in certain areas so that not all the information at every police force in every country is necessarily available to all others. I think one of the things that a new instrument could usefully do—and this is perhaps a deficiency of the general directive in the First Pillar and our own Act—is that it does not directly address disclosure or information sharing or information exchange. You get there by a roundabout way of adding together principles and in many ways that is the key to what we are talking about. An instrument which has a section on the sharing of information, exchange of information I think would be useful. That is actually something that is in this Council of Europe Recommendation.
Mr Thomas: I think it is also worth emphasising that the Recommendation is primarily aimed at harmonising the approach across Europe but it is not explicitly or specifically addressing cross-border exchanges. I think your particular questions are more concerned with problems coming out of cross-border exchanges. That is why I say, the general principles are the starting point but one may need to elaborate that for some of the cross-border matters.

Q263 ***Lord Wright of Richmond:*** My last question is to do with the joint supervisory authorities and I do not know which of you would like to answer. You referred to the fact that Europol, Eurojust, Schengen and the Customs Information System each have their own data protection controls and supervisory body. Would you see advantage in a single set of controls and a single joint supervisory board?
Mr Thomas: I think I will let David answer that one. I am about to become the chairman of the Eurojust JSB during the UK presidency next year but my experience is fairly limited and David has far more experience of these bodies.
Mr Smith: It might be helpful to separate out the two parts of your question: the single set of controls and the single supervisory body. I am not sure that it would be possible or desirable to move to a single set of controls because the Schengen System is different from the Europol System. I think what usefully we could have in a framework decisions are broad principles that apply across the board. You still need some specific rules for Europol and some specific ones for Schengen and so on. That does not mean that they cannot be supervised by one supervisory body. We would see a great deal of efficiency savings in that. The way it works at the moment is that we go to Brussels for two days every three months and the first morning we sit as the Europol supervisory body then in the afternoon we become the Schengen supervisory body. From the UK we send the same people but I have to say that some supervisory authorities do not even send the same people. There are different things to be discussed, but we could be much more efficient. We do not know enough about the legal processes but we think that to move to one supervisory body could probably be achieved before the EU Constitution is adopted; to give the work to the European data protection supervisor may require a step further. Maybe the framework decision will address this. The existing supervisory authorities have, for the first time, met together jointly and that is a trend which we welcome and encourage.

Q264 ***Lord Corbett of Castle Vale:*** I do not know if you know who we lunched with in Brussels last week, but I suppose in a sense by our invitation to lunch we actually created a joint supervisory board.
Mr Smith: That is absolutely right.
Mr Thomas: I think with the written memorandum which I mentioned earlier—they called it an Opinion—but I think your Committee has stimulated a coming together and it is very much appreciated. I had better not name the country, but I am told that one country asked, "Why are we addressing the House of Lords when it is a UK body?" The answer was, "It is a very distinguished committee which is taking matters very seriously" so

people were very happy to cooperate and collaborate on that basis.

Chairman: Thank you for those very flattering remarks, but we did find it extremely helpful; it was very interesting.

Q265 ***Earl of Listowel:*** How much specialist knowledge does the information supervisor need? For example, a children's home used to be inspected by an inspector who came from that background and now we have rearranged the system so that they are inspected by people who do care homes and various other institutions. Can you explain to me how that works?

Mr Thomas: I think we have to see ourselves as experts in data protection and freedom of information matters, not in the subject matter of the service providers, whether they are private or public sector service providers. Our expertise—whether it is resolving complaints, whether it is giving advice, whether it is promoting good practice, whether it is enforcing and regulating—is driven by our expertise in the subject of data protection. Having said that, we do have sectoral specialisations inside our organisation. We are currently organised in teams which look at particular sectors and have a good working knowledge of how things are done in that particular sector. David, for example, heads the team which is concerned with law enforcement, police, justice matters and a range of bodies which come under that remit. Yes, we need to have some expertise but I do not think we have to have people drawn from that particular sector. As it happens, we do have some ex-police officers on our staff and that is always useful, but I do not think that we need to be so expert that we know every detail of operational matters. Our job is to apply the principles and to challenge people to justify and explain what they are doing. If we are convinced by what they are saying, that may be acceptable; if we are not convinced then we will challenge them further.

Q266 ***Lord Avebury:*** Going back to a previous question, if there is a single joint supervisory body do you think there should also be a European Data Protection Supervisor as part of the new legal framework?

Mr Thomas: The supervisor already exists. Two years ago the post was created and he supervises the various EU bodies. Peter Hustinx is the European Supervisor. He already has an involvement in some of the matters that we are discussing this morning. He already, for example, attends the joint supervisory authority meetings. I think we have already speculated—and Lord Wright raised this possibility—that he himself might become the single supervisory body for these arrangements. I would not rule that out; David mentioned it as a possibility. I think that would probably require the Constitutional Treaty to be put in place first of all. There may well be a role to be played in this area but I think that may be racing ahead of making concrete proposals. I think we need to see the data protection framework first of all and we need to accept the principle that there should be independent supervision and how that is going to work and then we need to move on to who should be that supervisory authority. I do not want to go further this morning than recognising the option that the existing European Data Protection Supervisor could have that additional role tacked onto his existing responsibilities.

Q267 ***Lord Avebury:*** You mentioned just now that the Constitutional Treaty would have to be place for the new arrangements that we have been discussing. Are there any other implications of the Constitutional Treaty for the protection of personal data in the EU?

Mr Thomas: I have to be careful not to get into political territory; you are drawing me towards sensitive waters, Lord Avebury, and I do not want to get too far down that track! I would just make just a couple of points, if I may. First of all, the Treaty is significant, I think, in data protection terms. It contains a provision guaranteeing the right to data protection and explicitly refers to the existence or the need for an independent authority. In itself it refers to the Charter of Fundamental Rights which likewise, for the first time, spells out specific data protection rights going rather further than the Article 8 privacy rights in the European Convention on Human Rights. As I have understood it, as and when the Constitution is put in place, effectively that would abolish the distinction between First and Third Pillar matters but quite how that impacts on the matters we are discussing today—which may be a number of years down the track—I am not altogether clear. I do not think it in any way undermines the case we are making for a proper legal framework for the exchange of law enforcement information.

Q268 ***Earl of Listowel:*** What training is given by the information commissioners to law enforcement bodies on the exchange of information and data protection issues? You did mention earlier your role in advising and promoting best practice. Do you actually provide training?

Mr Thomas: I have survived two addresses to the data protection part of the Association of Chief Police Officers, one before Soham and Bichard and one after. So I myself have addressed their annual conference twice. David may elaborate more on some of the work which we have done with police forces around the country. Before David talks about training, I would want to make the point that we are

in constant contact with police forces and many of them have their own data protection officers and they are on the telephone to us perhaps two or three times a day with particular matters which they are raising. That is all part of the general support which we are giving. In the sense of more formal training David may want to elaborate.

Mr Smith: As Mr Thomas has said, we regularly speak at seminars we are invited to that are attended by the police and others. However, we do not have a formal training role as an organisation so we do not run training courses as such. Where we are asked to assist with police training we do. I have not been, but a colleague of mine has been to Bramshill and contributed sessions on training there. I think we are very much in the position that we are there if our assistance is needed. I would not want us to be seen as being over-critical of the police in the way they deal with data protection. They take the matter very seriously. Each force has its data protection officer. Amongst all the sectors of the economy we deal with the police probably have the best data protection setup—or one of the best data protection setups—and they do have their own internal training arrangements. I know training takes place and we are available, as I say, to assist if we are called on.

Q269 ***Earl of Listowel:*** May I just ask a further question related to that? With your experience in Europe do you feel equally confident that the police systems in Europe are adequately trained to manage information sensitively?

Mr Smith: I think what we notice is a difference in approach, but it goes back to some of the issues you talked about, about having a much more formal approach to data protection in certain of the European countries where—I hesitate to say exactly how they work—the approach of opening a new area for police investigation is a formal procedure where you open a file and you have it justified and those are the sorts of things that are checked. It is a much more procedurally based approach to data protection than we adopt here. They are sometimes less trained, I think, in making the judgments; it is more: if you follow the procedure it is okay, whereas here we look to see if the police comply and we really have to try to make some judgments as to whether they got it right and not just whether they followed the procedure.

Q270 ***Lord Corbett of Castle Vale:*** Can I just ask from your knowledge of the police forces' data protection officers, is this simply a matter of tick the box compliance or does it go into commitment in at least some of the 43 forces in England and Wales?

Mr Thomas: David's point was that they way things are done in this country does go beyond the tick in the box approach and I think it is taken seriously by police forces. I think sometimes it is seen as a constraint or a problem but I think they understand the importance of it. A lot of these issues surfaced during the course of the Bichard Inquiry. We did exchange quite fierce words with the police on one or two matters there, but I think we are very comfortable with the way in which Sir Michael Bichard drew conclusions from that. I think there has been a problem in some areas where the data protection officer is often a civilian—but not always—with quite a middle-ranking or junior position inside the police force and I think they sometimes struggle to have their voice heard. Having said that, I think right from the top all police forces do more than pay lip service to the importance of data protection but I think they would also say that on occasions they feel somewhat constrained or threatened by it. There are some quite severe misunderstandings. Bichard established that many police forces thought it was a criminal offence to get it wrong with data protection. Perhaps they have taken almost too seriously our warnings about the one criminal offence which does exist, which is individuals leaking information from police computers. That is a very serious matter but it is not directly relevant to the way police forces themselves handle personal information.

Mr Smith: I think that if there is to be a generalisation it is that those police forces where they have a direct route into senior management—chief constable, deputy chief constable, assistant chief constable level—achieve it the best; where it is part of operational thinking and management thinking, it is not just some technical add-on.

Q271 ***Viscount Ullswater:*** Mr Thomas, could I ask you to turn your mind to the transfer of data to third countries? You refer in your evidence to the need for any new legal framework to address international transfers of personal data. You also say that the principle established in the First Pillar in the Europol Convention is a sound one on this particular issue. What are the main data protection problems in the transfer of Third Pillar data from the EU to third countries or organisations?

Mr Thomas: I think I would start with the proposition that I put in my memorandum—that I think any data protection regime has to have some sort of provision relating to transfers outside the jurisdiction. That is why the First Pillar—the existing European Directive—but also the Europol Convention both have provisions relating to transfers. The general approach is that transfers are permitted if there are adequate levels of data protection in the receiving country. Obviously there may be some exceptions where there are matters of over-riding public interest, but the basic principle is that of adequacy. It is not the end of the story because, for example, one is

concerned that if you transfer information from country A to country B you have to have some further restrictions to stop that data being passed on to country C where there may not be adequate protection. One has to have some arrangements in place to safeguard that transfer. I think there are also strong arguments in favour of having as much centralisation of the determination of adequacy. That is why, within the First Pillar Directive, the European Commission has a role in looking at particular countries and determining whether or not the data protection laws in those countries are adequate or not. That is not to say that you have to constrain yourself or limit yourself to that situation: you can only pass information when there has been a central determination but that does make it easier for people on the ground. In the area of law enforcement one could contemplate a general determination saying that the laws in a particular country are adequate or one could contemplate a determination for a particular sort of transfer, transfers to this particular law enforcement agency, given that the arrangements within that particular agency are deemed to be adequate. The general point I am making is that one needs arrangements but one can be fairly flexible as to how they can be set up and applied in practice.

Q272 ***Viscount Ullswater:*** You have given us some concern, I think, about the reliability of information stored—whether it is in this country or in other countries—and we have talked about proportionality. Should the EU develop a common policy for the transfer of data to third countries and organisations? Should there be something about the ownership of the data, having some control over where it goes? I think you mentioned that if data is moved from country A to country B there should be some restrictions on moving to country C. Should there be some sort of ownership of data which has to be contacted before it can be transferred again?
Mr Thomas: I think the short answer to your question must be yes. It would be desirable as part of the package of measures coming forward to set out common policy for transfer to third countries or to organisations because I think that is in the interests of everybody. It is in the interests of the law enforcement bodies themselves to know were they stand; it is in the interests of citizens to know that there are safeguards for their personal information where it is being transferred. Going back to my previous answer, whether the policy would be directed at particular countries or at specific bodies inside countries I think is an open question. It may be very difficult to say that the United States—with perhaps a very large number of law enforcement bodies at the national, federal, state and local level—all of that is adequate. One may have to make a specific finding or a specific determination in relation to a particular authority. I speculate but the FBI, for example, might hypothetically be deemed to have adequate arrangements in place. I think the answer is yes, there are strong arguments for a common policy but I do not feel ready yet to articulate exactly what that policy should be.

Q273 ***Viscount Ullswater:*** What concerns me from what you were saying is that not only is data sometimes unreliable but it probably gets out of date relatively quickly and therefore is there a danger that when data is moved from one country to another it gets stuck in time and it is not updated and therefore could be accessed from a third country, which would actually be unhelpful in terms of information passed?
Mr Thomas: I would not want to say that is a matter of routine and the norm, but I think that is a very serious danger that you are highlighting. The answer is yes, so David may want to say a little more about his experiences at Europol where—I think he mentioned this in passing earlier—exactly that situation has arisen.
Mr Smith: It is probably second on the list of complaints from the Europol staff that we talked to when we did an inspection. The first is that nobody sends them any data and then when they do send any data they do not update it. I think it is understandable in some ways because Europol's work is analysing it, sending back information on suspects to member states. Member states then go off and arrest people and never bother to tell Europol that they have been arrested, for example. I am not sure what the magic answer is but I think that the point that you make about ownership may be a very good one, an important one to take on board. Maybe a difference in a Third Pillar instrument from a First Pillar instrument is that, when the data are transferred by a UK force or by NCIS to another country, they remain under the ownership of the UK police force maybe until such time as they are released, so there is an on-going obligation—a data protection obligation—to update the data that has been transferred.
Mr Thomas: If I could make a more general response to the question that Lord Ullswater has raised, I think it underlines the importance of what we call subject access, people being able to see their own files. There is nobody with a stronger interest in accuracy than the individual himself so although there are some exceptions—not least in the law enforcement area—the principle of being able to see your own files and ensure they are accurate and having the right to make corrections I think is an extremely important one. Again, we would expect to see that included in the package of data protection measures which we are talking about in this context.

Q274 ***Viscount Ullswater:*** Even with a Third Pillar usage.
Mr Thomas: Within the same sort of limitations as are available in this country. You do not have the same rights to see your police file as your credit card file, but you have some rights and we would expect the same sort of balances to be drawn in the law enforcement area, but the principle of access, not least for correcting out-of-date or inaccurate information I believe is very important.

Q275 ***Lord Avebury:*** In your original answer to Lord Ullswater you said that the principle underlying transfers to third countries was first that they had good data protection systems in place, but secondly that they would not further transfer the data to countries where there were no such systems. Does this not perhaps conflict with the necessity of transferring data to countries where there may be inadequate or no data protection regimes when the terrorist systems in operation in those countries—I am thinking, for example, of the central Asian republics where I doubt very much whether they have ever seen a PC—and yet there may be a strong argument for exchanging data with the police forces in those countries because they have more direct and immediate experience of terrorism than we do.
Mr Thomas: I understand the point you are making, Lord Avebury, and I think I was quite careful to say in my answer that there may be some exceptions where over-riding public interest considerations arise. I recognise that that sort of circumstance may arise and that is why I wanted to put that proviso in place. I think the example you have given may fall within that exception, but I would not want it to become the norm; I think that would only be in the sort of very serious matter which you are suggesting.

Q276 ***Lord Dubs:*** You have partly dealt with a point of issue in my question in your answer to the previous two, but I will ask it anyway. It is to do with relations between EU bodies and Interpol. Do you foresee any potential problems in the greater exchange of data between EU bodies and Interpol?
Mr Thomas: I have not had a huge amount to do with Interpol personally. It does have some data protection measures of its own but they are much weaker and much less robust than the sorts of matters we have been talking about this morning. I think the problem is not so much Interpol itself but what it does with the information. When it receives information it passes it on to others, which goes back to the sorts of points we have been discussing already. As I understand it, for example, there are no arrangements for independent supervision of the Interpol arrangements, only limited requirements for the familiar data protection principles to be applied in practice. It seems to me that if Interpol is to play a stronger role in these matters—we are talking now, of course, beyond European borders—then it needs, I would suggest, to bring its data protection arrangements broadly in line with those which apply not just across the European Union but also in the Asia Pacific area. When one looks at those parts of the world—looking also at South America—the approach which one now calls the European approach to data protection is becoming effectively the global standard. I am not including the United States in my comments because that is perhaps the exception, but Asia Pacific, Canada, the European Union, that is the global norm. Even in the United States, even though there is no federal data protection or privacy law, there is a very, very live debate about privacy and the protection of personal information. At both federal and state level there are many sectoral laws in the financial services area and in the health area. I was in Washington in February of this year and it is just as much a live debate and a live topic there as it is in Europe, notwithstanding the absence of a horizontal law such as we are used to in the European Union. I am sorry, I have digressed a little, Lord Dubs, but I wanted to make the point that Interpol, I think, needs to raise its standards in line with that global approach.
Mr Smith: Could I just clarify that Interpol itself has data protection arrangements and supervision. They might not be the same as in the EU but it is not that so much that is the issue. It is the arrangements that Interpol have with the countries that they transfer data on to and whether they come up to the standard. I think Interpol has a difficult job. If it imposed the sort of standard that we would like to see, hardly anybody would meet them at the present time and they would not function. I think the limited data protection controls in the system necessarily limit the effectiveness that Interpol can have. There is a limit to the information that can flow out through Interpol under the present arrangements. If it wants to be more effective then in some ways data protection controls go hand in hand with that, or certainly should do.

Q277 ***Chairman:*** I think, members, if you have finished the areas of questioning, could I thank both Mr Thomas and Mr Smith very much indeed for what they have given us this morning. You have shed light on an extremely complex area of concern, not just within the EU but we have gone global now. The clear and very open way that you have answered our questions has been most helpful. We are sure that some of your comments will be echoed clearly in our report and we do thank you very much, particularly I have been very grateful—and I am sure members would agree—with the examples that you have been able to give us. We always look for examples because,

in a complex report, that clarifies exactly what is happening out there in the real world. We are very grateful because they have been extremely helpful. Thank you both very much indeed; it has been a great pleasure to have you talk to us this morning.

Mr Thomas: Thank you for those comments.

WEDNESDAY 17 NOVEMBER 2004

Present	Avebury, L	Harris of Richmond, B (Chairman)
	Caithness, E	Listowel, E
	Corbett of Castle Vale, L	Wright of Richmond, L
	Dubs, L	
	Gibson of Market Rasen, B	

Memorandum by Paul Wilkinson, Professor of International Relations and Chairman of the Centre for the Study of Terrorism and Political Violence, University of St Andrews

1. Historical Background to European Cooperation against Terrorism

It was not until terrorism became a major problem for European Community states in the 1970's that the first significant steps were taken to strengthen European Cooperation against this modern scourge. Terrorism is predominantly a political crime. Traditionally the European democracies had all upheld the principle that in cases of political crime, extradition should not be guaranteed. This position was enshrined in the Council of Europe Convention on Extradition (1957). Under Article 3.1 of this Convention, a state party to the Convention could refuse extradition in cases where the offence for which extradition was being requested was a political offence or an offence connected with a political offence.

The first step towards abandoning this principle in regard to terrorist crimes came in 1977 with the European Convention on the Suppression of Terrorism which, at least on the face of it, requires ratifying states to apply the principle of *aut dedere aut judicare* (extradite or bring before your own judicial authorities) in the case of a terrorist offence or an offence connected with a terrorist offence. Yet a closer examination of the European Convention on the Suppression of Terrorism reveals that it is full of loopholes. For example, under Article 13 any state party to the Convention can refuse extradition if it chooses to view the offence involved as a political offence or an offence inspired by political motives. Also, under Article 5, the Convention allows a ratifying state to refuse extradition if it believes that the individual sought by the requesting state is likely to be prosecuted on grounds of race, religion, nationality or political opinion. These loopholes are clear evidence of the major weakness which has bedevilled all efforts to strengthen Euro wide cooperation against terrorism right down to the present: European states have been determined to retain their sovereign prerogative in matters of national security and law and order.

This is the central factor, in my view, which has obstructed the development of any genuine Euro-wide integration in the combating of terrorism and other forms of organised crime. Hence, it is not surprising to find that despite the significant development of a more integrated European economic zone under the Maastricht Treaty of 1992, with the free movement of goods and persons across national boundaries within the EU, matters of Justice and Home Affairs remained at a purely intergovernmental level, under the so-called Third Pillar.

Nevertheless there were incremental efforts to improve EU cooperation against terrorism throughout the mid and late 1990's. For example the EU Convention on Extradition (1996) obliged Member States to abandon the right to use political exemption as grounds for refusing extradition. The establishment of the European Judicial Network (EJN) in 1998 made it easier and faster to process judicial requests by one member state to another. The EU Convention on Mutual Assistance in Criminal Matters (2000) permits the transfer of telecommunication intercepts, and enables witnesses to give their testimony by means of video-link.

These modest though useful incremental changes were followed by more ambitious EU reforms at the turn of the century. Some of these changes have proved both prescient and highly relevant to combating the much greater terrorist threats presented by Al Qaeda, which were made so tragically evident by the 9/11 attacks. The EU Mutual Legal Assistance Convention (2000) obliges Member States of the EU to provide information on banking transactions, bank accounts and the monitoring of banking transactions. And although Eurojust, set up in 2001, has been viewed as a very modest measure to improve cooperation and coordination in the field of investigations, extradition requests and prosecutors, it is important to note that it has led to the development of potentially invaluable joint investigation teams, and the back up of a more comprehensive and valuable database to support law enforcement and judicial cooperation in both conventional organised crime and terrorist cases.

2. EU Counter Terrorism Measures since 9/11

The flagship of EU counter-terrorism efforts since 9/11 was the introduction of the European Arrest Warrant in 2002. The value of this measure to combat international terrorism is in theory all too clear. It would make the lengthy, cumbersome and unpredictable method of extradition between the EU states unnecessary. The EU Arrest Warrant is based on the principle of mutual recognition of criminal judgements of the courts of all Member States by fellow Member States. It becomes an administrative procedure, and is aimed at being a fast track means of transferring suspects. However, in practice, the European Arrest Warrant, which was supposedly to come into force from January 2004, has been somewhat undermined by the reluctance or unwillingness of some key member states to ratify it, and by the continuing desire of certain members states to maintain total national political control on these matters. At time of writing the following member states had still failed to enact the European Arrest Warrant: Italy, Germany, Greece, Czech Republic and Malta.

As in the past, however, the pressure of events has conspired to push the EU into greater counter-terrorism activity. The most recent catalyst was the Madrid bombing on 11 March 2004, which killed almost 200 civilians. This led the EU to launch an ambitious Plan of Action to Combat Terrorism (March 2004). The strategic objectives of the Plan are as follows:

- To deepen the international consensus and enhance international efforts to combat terrorism.
- To reduce the access of terrorists to financial and other economic resources.
- To maximise capability within EU bodies and Members States to detect, investigate and prosecute terrorists and prevent terrorist attacks.
- To protect the security of international transport and ensure effective systems of border control.
- To enhance the capability of the European Union and of Member States to deal with the consequences of terrorist attack.
- To address the factors which contribute to support for, and recruitment into terrorism.
- To target actions under EU external relations towards priority Third countries where counter-terrorism capacity or commitment to combating terrorism needs to be enhanced.

This Plan was accompanied by an EU Declaration on Combating Terrorism, a powerful statement of solidarity against terrorism in the wake of the Madrid bombings. The European Council stated it was "deeply shocked by the terrorist attacks in Madrid and expressed its sympathy and solidarity to the victims, their families, and to the Spanish people. The callous and cowardly attacks served as a terrible reminder of the threat posed by terrorism to our society".

3. The Role of Intelligence Data Exchange in EU Counter Terrorism Activities

The EU Declaration on Combating Terrorism can be seen as a powerful call for solidarity and firm action from Member States, but it is clear from the language of the Declaration and the Plan of Action that the call for action is primarily directed at the Member States own national authorities, because in reality it is they who have the power and resources to carry out the Plan. It is true that under Objective 3, the Plan speaks of enhancing the "capacity of appropriate EU bodies (ie Europol, Eurojust and the Police Chiefs' Task Force) in the preparation of intelligence assessments of all aspects of the terrorist threat . . .".

However, the key source for this intelligence is inevitably the secret intelligence services and police forces of the individual Members States. The reality is that national governments are unwilling to allow other governments' intelligence services and police anything more than a limited access to their secret intelligence on terrorism [or indeed on other key security issues]. There are a number of reasons for this:

- They are afraid of disclosing their sources and possibly compromising them.
- They do not trust other countries to keep the secret intelligence secret.
- They fear that other countries might take action on the basis of the information given to them, which would be contrary to the sending State's interest.
- They are afraid of revealing gaps and errors in their intelligence, which an unlimited access would disclose.
- In the extremely competitive world of intelligence, agencies are reluctant to part with intelligence, which they assess as giving them an advantage over their rival agencies within their own nation state.

17 November 2004

For all the above reasons national intelligence agencies working with Europol and other EU collaborative bodies will only provide sanitized intelligence data for sharing purposes. Hence it is national governments and not the EU, which inevitably and understandably are the key recipients and gatekeepers for sensitive counter-terrorism intelligence. When they do engage in serious international cooperation it is almost invariably at the bilateral or trilateral level. When there is a well-established and trusted bilateral cooperation, as between France and Spain in regard to Basque terrorism, there will be a concomitant sharing of high grade and sensitive intelligence.

This does not meant that intelligence sharing at EU level is a waste of time. It may have a valuable part to play in developing threat awareness and vigilance in Members States. And, although access to raw intelligence data will inevitably be restricted by the collecting authorities' national governments, we should bear in mind that the sharing of analyses and assessments may be highly beneficial in persuading national authorities to provide enhanced or more urgent action in support of a threatened or victim state.

In the light of the above, I support the 8 June proposal by Javier Solana, EU High Representative for the CFSP for charging the EU's Joint Situation Centre (SITCEN) with the production of intelligence analyses with a view to support EU policymaking.

In his statement at Luxembourg on 8 June 2004, Javier Solana reported that the Heads of the Security Services of the Member States have given their support to the proposal and that he hoped to reach "a final consensus on the proposal in the next European Council". Mr Solana correctly pointed out in his statement that his proposal would "build on the existing cooperation within the SITCEN, established between the external intelligence services of the Members States since early 2002".

Mr Solana put forward what he termed "core ideas" which he hoped the Council would endorse:

1. Moves by the Heads of the EU's 25 Security Services to meet regularly together as a group in the format of the existing Counter Terrorist Group (CTG).
2. The work of CTG would allow for close cooperation in the field of analytical exchange between Security Services, and would provide scope for improved operation cooperation.
3. Moves by the European Police Office (EUROPOL) to reactivate their Counter-Terrorist Task Force and efforts to improve the flow of criminal intelligence to EUROPOL.

Mr Solana argued that these measures would mean that:

1. EU decision makers would be better informed, inter alia, about threats, terrorist methods, organisation of terrorist groups and thus better prepared to devise effective EU counter terrorism policies.
2. Member States would receive better support from European bodies. They would get assessment material from the EU's SITCEN and their police services in particular would get better support from EUROPOL.
3. Member States would retain the lead in the operational field but would be working more closely together through CTG, EUROPOL, as well as through existing bilateral arrangements to strengthen information exchange and cooperation.

I fully accept the logic of Javier Solana's proposal. It is realistic in recognising that Member States will retain the lead in the operational field and that his proposal, if implemented will simply complement "existing bilateral arrangements".

However, there is an overwhelming counter-terrorism case which Mr Solana does not deploy but which should persuade all Member States to adopt his proposal. The threat from the Al Qaeda network is quintessentially transnational. As we saw in the investigation of the Madrid bombings and many other acts of the Al Qaeda networks and its affiliates, the terrorist cells and their support networks operate across national boundaries. We need to greatly improve our transnational networking in order to prevent and combat Al Qaeda, the most lethal network in the modern history of non-state terror.

To sum up: the EU has made small and often faltering steps towards greater counter- terrorism cooperation. The role of national governments and their counter-terrorism agencies and their bilateral cooperation with other States' authorities have made a far more significant and effective contribution. But, 9/11 and 3/11 have had the effect of triggering a more proactive approach by the EU. We should, in my view, warmly encourage this approach, viewing it as a way of adding to our existing methods of cooperation. Because of the changed nature of the threat it could develop into something very useful. I hope that Her Majesty's Government will encourage, and contribute to this process.

17 November 2004

There are other measures which the EU has already initiated or is proposing to initiate which I believe to be urgent priorities in the fight against international terrorism and which the EU is particularly well placed to push forward:

— The inclusion of biometrics in passports and the strengthening of European border controls.

— Efforts to get Member States to adhere to the commitment they made in the EU Action Plan for Combating Terrorism, especially implementation of the European Arrest Warrant and Joint Investigation Teams.

— Facilitating joint training for police and emergency services.

— Enhancing EU capabilities for combating terrorist financing and money laundering.

24 November 2004

Examination of Witness

Witness: PROFESSOR PAUL WILKINSON, Chairman, Centre for the Study of Terrorism and Political Violence, School of International Relations, University of St Andrews, examined.

Q278 ***Chairman:*** Good morning, Professor Wilkinson. We are most grateful to you for coming to talk to us this morning. Thank you very much indeed for your paper and the evidence that you sent which was extremely helpful to us. I am sure, through our questions, you will be able to help us even further. I must register for the benefit of any members of the public who are going to be listening to this, the subject of our inquiry which is an examination of a number of proposals designed to strengthen EU counter-terrorism activities, particularly through much more extensive data exchange. These proposals raise important issues relating to, among other things, data protection and the institutional arrangements within the EU for combating terrorism. The interests of members that are relevant to this inquiry are placed at the back of the room and I understand that you have had a copy of those, Professor Wilkinson. I wonder if you would like to make an opening statement and then we can launch into questions.

Professor Wilkinson: If I could start by explaining a little about where I come from for those on the Committee who may not be aware. I am Chairman of the Advisory Board for the Centre for the Study of Terrorism and Political Violence, which is a registered research centre at the University of St Andrews under the umbrella of the School of International Relations. Although my chair is in international relations, my specialist research area for about 35 years has been the study of terrorism, particularly concentrating on the problems of democratic response and the problems of international co-operation. That work has been going on through the work of the Centre which was established in 1994, so it is actually our tenth anniversary this year.

Q279 ***Chairman:*** You now know why we invited you; we heard you were the very best person to come to talk to us.

Professor Wilkinson: You are very kind. There is too little research I suggest going on in this area and we are doing what we can but we have quite a small full-time staff, a lot of extremely good interns who are very bright, covering all the major languages in the world, which is a great advantage. We are independent; we are funded by research grants from various bodies; the biggest grant at the moment is for a project which I am directing which is on the preparedness of the United Kingdom for future terrorist attack. We are nearing the end of that project. That has been in combination with the Mountbatten Centre at the University of Southampton. Professor John Simson, Frank Gregory and colleagues there are an extremely important part of the team. I have been doing work with the Institute of Security Studies in Paris which, as you know, works closely with the European Union and the Commission. I have been commissioned to do a paper on European Union future response, so the invitation to come here came at a time when I had already been thinking closely about these matters. That tells you a little bit about what we do. My director's name is Magnus Ranstorp; many of you will know him because he appears regularly on television and gives beautifully clear explanations of the threat in the Middle East and so on. His specialism is the Middle East area. That gives you an idea of the scope of our Centre.

Q280 ***Chairman:*** I think that fits very neatly with my first question, so it has been extremely helpful. I wonder if you could elaborate on how you work in the counter-terrorism field.

Professor Wilkinson: There is an amazing amount in open sources. Because we are independent and academic we obviously do not have access to classified material but if you scan the internet—as all of you will be doing—it is amazing what is publicised on the internet, from statements by the propaganda

groupings, political wings of extremist organisations to government sites such as the MI5 site, which has become very useful recently to members of the public who want to know about the security threat to Britain. There is also information about new technologies. One of the advantages to academics is that we have access to all that information in the open sources; unfortunately, the terrorist organisations also do and they study these things and they really are getting very sophisticated, as you know, in using the new information technology and in finding out what they need to know about, for example, vulnerabilities in the national critical infrastructure, about the coming events which they might want to target and, of course, the kind of weapons they can use. It is a sad fact that if you know where to look on the internet you can find the formula for pretty well any weapon of chemical or biological nature that could be extremely dangerous in the hands of terrorists. The information revolution has actually made our job in terms of combating or preventing terrorism that much more difficult.

Q281 ***Chairman:*** We all recognise that and it is exchange of data which is one of the areas which concerns us most at the moment and we will ask questions around that. Can I ask how, from your perspective, you feel the terrorist threat and the response to it has changed in recent years? In your paper you talk very clearly about 9/11 and what happened from then, but how has it affected the work that you do at the university?

Professor Wilkinson: Going back to the 1970s and 1980s when I was researching at the University of Wales and then later at Aberdeen University it was regarded as a serious problem by countries which had a major internal problem, for example the United Kingdom or Spain. It became a problem for those countries with the fighting communist organisations—, the Red Brigades, the Red Army Faction in Germany and so on. However, it was never a problem of such strategic concern that it was pushed to the top of the agenda; it remained, as one of my colleagues, the late Professor Hedley Bull (who was a very distinguished international relations specialist) a law and order problem, a minor problem for governments rather than a problem for the international community. It is interesting that many international conferences at that time did not figure terrorism in the agenda; it was not regarded as an important subject. However, by the mid- and late-70s after the beginnings of many different kinds of terrorism—Middle Eastern terrorism stimulated by the Israel/Palestinian conflict, the fighting communist organisations beginning to launch a series of attempted assassinations and attacks in Europe—the Council of Europe (which has traditionally, as you know, taken a rather interesting role in trying to harmonise laws in Europe) took an initiative with the European Convention on the Suppression of Terrorism. That was an interesting act because it was the first time that the European countries collectively decided that this was a problem that required some wider action by all European states acting together. Unfortunately, as I explained in my paper, it was a rather empty gesture in some ways because in order to get the thing agreed and ratified by the member states of the Council of Europe they had to make all kinds of caveats. If you look at the caveats you could drive a tank through them really and so a country could decide to regard a particular event as a political crime even though other countries in the Council of Europe regarded it as an obvious deliberate attempt to use terror as a weapon. That was a faltering step and I would have generally described the early progress in the European Union response as a rather faltering but incremental response. As they became aware of the more serious implications of terrorism and the terrorists themselves became more destructive in the 1980s—but particularly in the 1990s—you then get a rather major output of measures designed to strengthen co-operation and with some effectiveness, such as the Mutual Assistance Convention, such as the means of tackling the financing of terrorism which was strongly supported by the major European Union states. This is, you must remember, well before the 2001 events of 9/11, so the European Union was certainly incrementally and very slowly moving towards a stronger international approach to co-operation. It was taking rather important steps in the 1990s and there were good reasons for this. You will recall that it was a decade in which there were some really very lethal, highly destructive terrorist attacks, for example the Oklahoma bombing, the first attempt on the World Trade Centre in 1993, which was a failure in terms of killing large numbers of people. We now know that they did want to kill large numbers of people, they wanted to tip the tower; it just technically did not work out for them,. It is certainly clear that a number of groups decided that they wanted to go for spectacular headlines with particularly bloody attacks, for example the Baruch Goldstein attack on the mosque in Israel which had very serious consequences for the peace process (although there were a lot of other reasons which undermined the Oslo Accord, it was certainly one of the factors); the Buenos Aires attacks on the Israel Embassy and on the charity headquarters in Buenos Aires. All these were on a scale which was much more serious and the range of attacks over a wide range of countries I think persuaded European leaders that they needed to take the threat very seriously. Then of course closer to home we had the concerns about the Northern Ireland situation and whether we would be able to bring about a successful conclusion to the

discussions on a ceasefire and a peace process. There was great pressure within the European Union to strengthen cooperation in all these respects: political, diplomatic, addressing the roots of terrorism and the security aspects and improving security co-operation with the police and judicial cooperation. However, the really big break through in terms of a desire to do something rather more comes rather inevitably after 9/11 which was unprecedented in terms of the lethality of the attacks. In one single day you had more people killed in the United States than had been killed in the entire Basque terrorist campaign against the Spanish state. That does put it into perspective. More people were killed than were killed in the attack on Pearl Harbour. There were a very large number of civilians killed, so inevitably countries throughout the world began to look to this sign of much more serious terrorist capability as a threat of a strategic nature. I think they are right because clearly the Al-Qaeda movement which was responsible for this attack and its various affiliated organisations does have the explicit aim of killing large numbers of civilians and that is contained in the so-called fatwa issued by Bin Laden for the World Front for an Islamic Jihad, in which he explicitly said that it is the duty of Muslims everywhere to kill Americans, their allies—including civilians—whenever and wherever the possibility arises. Therefore you have a rather different kind of response necessary when you are dealing with such a ruthless and lethal organisation. Organisations that we faced in the 1970s and 1980s, although they certainly committed some awful violations of human rights, did have some sense of restraint. They were political in the sense that they wanted to garner some support from their constituency—they did not want to throw away that support—and they must have been aware that by, for example, poisoning the water supply or launching some kind of chemical or biological agent that would cause mass casualties, that would hardly have endeared them to the people in their own communities to whom they were looking for support. The more political minded secular groups of the 1970s and 1980s wanted to use terrorism, as Brian Jenkins has said, to get a lot of people watching rather than a lot of people dead. However, the Al-Qaeda movement is decidedly interested in getting both a lot of people watching and a lot of people dead, as we have seen in so many of the attacks this movement has been responsible for since 9/11. Although fortunately they have not succeeded in doing anything since of that scale they are certainly capable of killing hundreds of people in individual attacks as we saw with the Madrid train bombings. I think the reason why the European Union responded so strongly to the 9/11 events was a very logical, very sensible appreciation of the much more serious level of threat that we now all face. Naturally there are no immune countries in the European Union. Although some governments may feel that they are rather more immune I think that is a dangerous illusion; they are really fooling themselves if they think that Al-Qaeda is really interested in giving immunity to countries which are seen collectively as part of an enemy.

Chairman: I know Lord Wright wishes to say something at this point. We do not have very much time this morning unfortunately so if I could invite members to keep questions fairly limited, please.

Q282 ***Lord Wright of Richmond:*** I will ask a very brief question and invite you to give a very brief answer. Professor Wilkinson, you referred to some measures which would hardly have endeared terrorist groups to their supporters. How do you explain briefly the murder of Margaret Hassan?

Professor Wilkinson: I think that the group that carried out that atrocity clearly did not care about the public opinion response, the public opinion dimension. To some extent the Islamist groups do care to the extent that they want to try to build up support. They would make a great mistake, I think, if they ignore public reaction to their activities and they did make great mistakes in Saudi Arabia, in Turkey and in Indonesia. We see parts of the population becoming highly critical of what they see as weak responses by governments and demanding much stronger responses because fellow Muslims are dying at the hands of this group that claims to be championing their religion. This clearly does not make any sense and they have become very angry and are demanding stronger measures. I think in the case of the group that has carried out the atrocity in Iraq it may well help the more moderate forces in Iraq who want to say, "Look, we recognise that this is simply totally unacceptable. Whatever the cause, whatever your political argument, nothing can justify anything like that." It is rather like the Beslan school massacre in that respect; it is totally beyond any kind of moral justification.

Q283 ***Lord Corbett of Castle Vale:*** Professor, in your paper you speak on the one hand about Europe-wide integration and in the next paragraph EU cooperation. Is it either/or, or a combination of both in the real world.

Professor Wilkinson: In the real world, as you probably guessed from the language of my brief, I would regard myself as a liberal realist; I am not a liberal utopian. I think the integration within the European Union has been surprisingly effective in the economic and social sphere but surprisingly slender in the area of foreign policy and security. The implication in my paper is really that whatever the European Union does, if it is doing good sensible things, it has to recognise that the leading players are

still the national governments and the national security agencies. I think that Mr Solana's proposals are realistic in the sense that he recognises that that is where the lead remains and is likely to remain for a very long time ahead.

Q284 ***Lord Dubs:*** Professor Wilkinson, in the different EU states there are significant differences in legislation and culture. To what extent do these differences hinder international cooperation on anti-terrorist measures?
Professor Wilkinson: They have been a handicap in the past. for example, the different procedures on extradition which are inherent in our different legal systems: in some countries as you know you virtually had to have a kind of pre-trial—a trial before the trial in the requesting state—and that was something that would take a very long time. That was one of the factors which I am sure led the European Union ministers to think in terms of a European arrest warrant as a possibility. I think that the fact is that legal differences between the national states have often limited the amount of cooperation that could actually be achieved. We are still seeing some effects of that. I mentioned in my paper the difficulty in getting implementation of the European arrest warrant, which is partly a cultural thing if not legal; it is a reluctance on the part of certain countries to go as far, as it were, in trusting—in the context of this idea of mutual recognition—the decisions of the justice systems of another country. That kind of scepticism and distrust is something which the European Union has always had to contend with but especially in the field of law and order and security co-operation. I think it remains a problem that is, if you like, inherent in the whole European Union project. However, I am a realist and a pluralist and I believe that although those are difficulties we can overcome them by accepting that nation states are the lead players but using the fora that are provided in the European Union—and they are very useful fora, now much larger, of course, since enlargement—to create a greater awareness and a more realistic awareness of the nature of terrorism and the threat of terrorism and of other problems. I think that the other benefit of having these fora is that you can bring together the police chiefs in the Police Chiefs Task Force, the heads of the security services under the framework of the counter-terrorism group and so forth. I do not mean to imply in my paper that these meetings are not useful; they can be very useful in agreeing on things where there is a consensus within the wider European Union and that can carry us forward. However, there will be occasions when there will be deep divisions and it will be then up to the nation states to take the measures they think are necessary.

Q285 ***Lord Dubs:*** You referred to enlargement; what do you think is the impact of enlargement on the capacity of the EU to deal with counter-terrorism?
Professor Wilkinson: I think it is going to make the whole problem of decision making much more challenging and probably prolonged because of the large number of different national interests and national considerations involved. I think it was difficult enough prior to enlargement but it is going to be even more difficult when you are dealing with such a large grouping of countries. On the positive side, if we do get agreement on something like a new legal arrangement like the European arrest warrant, then if it applies over such a grouping it is all the more effective because it is working over a wider area involving far more judicial co-operation. Again, I am a realist; I do not think we are going to find it easy to arrive at these consensual decisions, but where we can get some consensus then we can move forward through the European Union and we can do certain things in the European Union—I would go so far as to say—which cannot really be so easily achieved at bilateral or trilateral level. At operational level it is bilateral cooperation that has historically been the most effective and successful way in which governments and security agencies have combined against terrorism. Look at the co-operation between the Spanish and the French authorities in whittling down the violence from the ETA movement. I think that if we are looking at creating arrangements which will deny resources to terrorism such as agreement on financial measures to exchange information about banking transactions and so on, that is very important because the financial intelligence that you can get from those kinds of things may lead you to identifying the terrorists; it is a very valuable intelligence asset. If you can get agreement on those rather unglamorous, little noticed aspects of combating terrorism, then that is progress. I am happy that we can achieve that through cooperation, through the European Union, where we can achieve it.

Q286 ***Earl of Listowel:*** Professor Wilkinson, how important is the training of law enforcement officers in enhancing Member States' counter-terrorism capacity? In answering that question perhaps you could also speak to the question of language across Europe—you mentioned this earlier in your introduction—and perhaps the development of a common format in the gathering of information, if that is relevant in your opinion. Also, the funding of exchanges of officers from one country to another which is perhaps related to the language question.
Professor Wilkinson: Thank you very much for that question because I am a great believer in joint training and exercises which I think are a very practical way of training for both the police and the

other emergency services that might have to deal with terrorism events. If we bear in mind that some of the things we have to worry about from a network like Al-Qaeda could simultaneously affect the population on one side of a national member state border and on the other side of the border—so you cannot inevitably predict that each event is going to be confined to a particular member state frontier—it may be something which they all need to collaborate on. Then joint exercising and joint training become all the more important and you can create a more common culture—raising the point which was made by a member earlier—it really is important to develop that common culture of co-operation not only in a greater awareness of the problems but also how other people work within the European Union in order to better understand how to cooperate effectively. I have had a little experience of this in the Irish context with conferences involving people from north and south of the border and mainland police forces for that, and so on. It is extremely effective; it gradually improves the spirit of co-operation. It is very good for creating personal links which, as you know, at the end of the day are so important in bilateral and trilateral cooperation. There is an enormous amount of benefit to be had from the joint exercises in training. Recently in Tulliallan, the Scottish police college, we mounted a joint leadership course in counter-terrorism which involved the Canadian RCMP, the police service of Northern Ireland, the Irish police, the UK mainland police (both Scottish and English) and the FBI (so there was an American dimension as well), so there was a pretty comprehensive grouping. It went very well; the feedback from the students was extremely favourable. If it can work among those very different countries, I think it is clear that you could make this work at the European Union level as we cooperate so successfully in a lot of other areas. I think the idea of a European police college is an excellent idea and we should develop it by supporting joint training and joint education, and language training of course would be a valuable part of that because if you are looking at border controls—something I mentioned in my conclusion and something which is very ripe for greater action I think—then one of the great deficiencies we have in our immigration service and the services that have to try to deal with border control is a language deficiency. I think we could certainly benefit enormously in that respect. In joint investigations one of the very good developments since 9/11 has been the development of the idea of joint investigative task forces. In the Madrid bombing you have a very good example of the need for that co-operation because there were links, if you recall, between the people who planned the bombing in Madrid and people based in other European countries and they were all extremely helpful. That can be best organised when you have a joint structure for investigation. That is another example, I think, of a positive thing that you can do through the European machinery.

Q287 ***Lord Wright of Richmond:*** Professor Wilkinson, I think your reference to co-operation and your warm endorsement in your paper of a more pro-active approach by the EU probably answers my next two questions. First of all, on the adoption of exceptional counter-terrorism measures, are there measures both in our own legislation and in EU regulation that you think are not justified by the increased terrorist threat? Secondly, the Commission's proposals to facilitate the exchange of data between law enforcement authorities: I think the implication of your paper is that you welcome that, but is there anything in either of those fields that you think is not justified?

Professor Wilkinson: I do not think so. I think at the moment if you are looking at, for example, implications for civil liberties, the national government's response and the national legislation and the actions of security forces within national borders should be the main target, if you like, for those who are concerned with ensuring that there are no unnecessary infringements of civil liberties. I believe—and I have written about this on many occasions and I strongly believe it in terms of the experience of fighting terrorism—that despite the greater threat to be faced from Al-Qaeda we do not need to suspend a rule of law in our observance of human rights and democratic process in the name of greater security. I think that is a great mistake. To cross-refer to another inquiry which Parliament launched into the Blunkett measure—the Anti-Terrorism, Crime and Security Act of 2001—I did, with other academics, express strong reservations about the fourth section of that Act which, as you know, deals with detention without trial. I know it affects a small number, but the principle is important and I still believe that if we gave the police sufficient resources they could actually mount the monitoring which would then lead to evidence and you could use the Terrorism Act 2000 (which is in conformity with the European Convention on Human Rights in my view) if you find they are involved. However, if they are not involved, just to put them in prison and throw away the key does seem to me to be a great mistake.

Q288 ***Lord Wright of Richmond:*** Do you have any reservations about data exchange between law enforcement authorities?

Professor Wilkinson: I do not because within the European Union as a whole I think there has been a rather less draconian response—if I can put it that way—in terms of the nature of the laws they have passed. They are, from my understanding, in

accordance with the requirements of the European Convention on Human Rights and I think that should be our guideline. If we are having to derogate from important principles of human rights in the Convention and other members of the European Union are not, we should be asking ourselves, "What are we doing or what are we not doing that really necessitates that? Should we not try to get into step?" because I think the European Union's concern about human rights matters is well known. I would, however, just add the rider that I think that the European Parliament should be expending more time on scrutinising the security cooperation measures because that, is very much their task as a European Parliament and I do get the impression that they have been rather peremptory in the way they have approached security measures.

Q289 ***Earl of Listowel:*** There is an issue, a tension, between being parsimonious with information and also having enough soft information to generate a profile of people. Where do you stand on that? Are you concerned that not enough information is transmitted or do you feel that it is about right at the moment?
Professor Wilkinson: I think from a realistic perspective if one talks to people in government and in the security services it is simply not going to happen, to have a kind of free access to the full intelligence which each nation state is going to have on terrorist organisations. It is just not going to happen. Countries are too jealous of their national prerogative in terms of their secret intelligence. I listed some of the reasons for that in my paper: the danger of compromising sources, the worry about another state misusing the information in some way which would be counter-productive and so on. Some of these are very logical and very understandable reasons. In my view it would be difficult to be the first country that heroically threw away all these safeguards on national security hoping for the best within a European Union which is not yet a European state. It would be very reckless to throw away those precautions but I think there is room for sharing analytical assessment. This is different from divulging all the details of names, addresses and circumstances of a particular on-going investigation; this is a question of distilling the information that you have in your intelligence community and providing really good quality assessments that are going to be useful for your allies within the European Union. We do that in our relations with the United States of course already, and with Canada and other close allies. We do it on a bilateral basis with the French who have been extremely helpful, by the way, in counter-terrorism intelligence because they know so much about the Middle East. However, on the European level, in my view, there is room for sharing threat analyses, analyses of trends and developments in terrorism and that is my understanding of what Mr Solana really expects; he does not expect a kind of portcullis to go up and everybody to agree to allow full entry to the secret tower of the intelligence community. I do not think he is envisaging that at all. What he is working for is greater collaboration, sharing of ideas, bringing people together to discuss possible pan-European efforts. I think that is a very sensible position. His experience in NATO gives him that realist background.

Q290 ***Lord Avebury:*** When you talk about sharing analytical assessments do you think that enough has gone on at the European level concerning the ideological basis of terrorism? I do not know whether you have read Jason Burke's book on Al-Qaeda but I was very much impressed with that as an analysis of the ideological foundation from which terrorism springs. It seems to me that, unless you understand that, you are not in a position to take the detailed action that states in particular have the power to do. Do you think that enough goes on at European level in relation to sharing that sort of analysis?
Professor Wilkinson: I do not think it does and I do not think it does at national level. I agree with you; I think it is important to try to understand the roots of these terrorist campaigns and the conflicts which are often much broader which spawn terrorism as a by-product. The Israeli/Palestinian conflict would be a good example. I think there are ways in which the European Union is already trying to address some of those conflicts to reduce the reservoir of people who might be willing to become suicide bombers. The European Union has been very strongly out in front in asking for greater international effort and promoting greater international effort at revitalising the Israeli/Palestinian peace process. I believe we should continue to be urging that because although that would not end international terrorism magically—it is unrealistic to expect that it would; these people often have other motivations for continuing with terrorism—it would greatly reduce the reservoir of young people who would be willing to do this kind of thing. It reduces one of the major grievances or injustices which they are concerned about. We should be making progress on what I would call corrigible conflict situations but at the same time recognise that there are some incorrigible situations. I do not think you can regard Bin Laden, for example, as an interlocutor whom we should invite to a meeting with the European Union and say, "Now, Mr Bin Laden, what would it take to stop you promoting mass killing and bombing attacks?" It would be as absurd as the Japanese prime minister, after the Aum Shinriky nerve gas bombing in Tokyo, inviting Asahara, the leader of the Shinriko group, into his office and saying, "Now, Mr Asahara, just

tell me what kind of deal we should do to get you to abandon this?" A democratic government cannot do that without betraying their citizens and their fundamental principles. That is why law enforcement, rule of law, international intelligence cooperation, is really the best way of dealing with these extremely incorrigible situations.

Q291 ***Baroness Gibson of Market Rasen:*** Professor Wilkinson, you obviously believe in co-operation but I am wondering if you think there are limits to co-operation between law enforcement authorities and intelligence agencies.
Professor Wilkinson: Yes, I think there are some very strict limits. I do not think that any of the intelligence agencies or police forces in Europe would be prepared to give a totally free access to other agencies, even within their own country. This is the big thing that people are perhaps not aware of. It is not a question of agencies already sharing everything within their own state because they are concerned about the possibility of information being misused or problems of that kind—we know there is a traditional tension between uniformed and non-uniformed sections of the police and security services—and that will continue to be a realistic factor which we have to reckon with but that does not mean that we should give up on co-operation and somehow imagine that what European Union organisations do is not relevant to us. It can be extremely helpful in creating the awareness that we have been talking about and the problem that Lord Avebury raised of creating a greater European energy to do something about the basic conflicts which are spawning terrorism. The European Union is potentially an extremely helpful body for us, it is just that the lead role for dealing with the security aspects is going to remain with the nation states for a very long time ahead.

Q292 ***Lord Corbett of Castle Vale:*** That said, Professor Wilkinson, there is a proliferation of agencies in both formal and informal structures within the EU dealing with counter-terrorism. Do you see a need for better co-ordination and streamlining of these bodies? Secondly, do you think they should all be brought formally within the EU structures?
Professor Wilkinson: I do not think that it is realistic to bring them into the European Union's structure. I think they will remain essentially inter-governmental fora because of the factors that I have described, but that does not mean that they cannot be useful or that we should be reluctant to cooperate with them.

Q293 ***Chairman:*** Could I have a final word about your views on the role of the Counter-terrorism Co-ordinator?
Professor Wilkinson: I am due to meet him very shortly so I must be careful what I say. I think the idea of having a co-ordinator is an excellent one. I will reserve judgment on what the impact is going to be. If we judge by the impact of our own co-ordinator on these matters, Sir David Omand, he has been a superb man at getting co-ordinated action in this area. I think that if we had a kind of equivalent person in the European Union it would be marvellous; someone who knows their way round the system. Of course Sir David had experience in so many relevant ministries before taking his present position so he is ideally placed. I will reserve judgment on whether the new European Co-ordinator is going to energise European coordination in the same way.

Q294 Thank you very much indeed, Professor Wilkinson. I am terribly sorry that we have had such a dash through because I know we would have much preferred to spend a lot more time asking you many, many more questions. Could I, on behalf of the Sub-Committee, thank you very much indeed for coming and sharing your views with us and for the very interesting paper that you submitted.
Professor Wilkinson: It has been my pleasure.

WEDNESDAY 17 NOVEMBER 2004

Present	Avebury, L	Harris of Richmond, B (Chairman)
	Caithness, E	Listowel, E
	Corbett of Castle Vale, L	Wright of Richmond, L
	Dubs, L	
	Gibson of Market Rasen, B	

Memorandum by Statewatch

Justification

Q: *Does the fight against terrorism require much greater operational co-operation and freer exchange of data between law enforcement authorities (both national and EU)?*

In our Scoreboard produced in March 2004 we identified 56 proposals in the EU counter terrorism plans that followed the Madrid bombings. Our analysis found that 27 of these proposals which were a danger to civil liberties or had little to do with combating terrorism. This is available at: http://www.statewatch.org/news/2004/mar/swscoreboard.pdf

There have been a number of developments since this was published.

Exchanging Information on Terrorist Investigations

There certainly is a need for greater operational cooperation between law enforcement agencies in the fight against terrorism. However, this cooperation should a) be limited to terrorism and b) ensure that the rights of suspects are observed.

For example, the Commission proposal (COM (2004) 221) provides for the information gathered during the investigative phase being communicated to Europol, Eurojust and agencies in the 25 member states.

It is sensible that such information should be made available. However, the proposal contains no provision for the "information" to be removed/deleted should a person be found innocent. There is no provision for the "information" passed over on those caught up in a "criminal investigation" but never charged or convicted to be removed/deleted. This is especially worrying as an "investigation" into a suspected terrorist offence would embrace not just the subject but their family, friends and work associates to see if there were any links to the suspected offence. A typical investigation could involve 20-40 other people who are found to be quite innocent but "information" on them could be "immediately" transmitted to dozens of agencies across the 25 EU member states.

In April 10 Muslim "suspects" were arrested in the north of England but never charged—this could have led to several hundred names and personal details being put into EU-wide circulation with no obligation for this data to be deleted. If there is no obligation to delete the names and details of innocent people they could find themselves on "watch-lists" for years to come.

There is another problem with the draft Decision. The intention is to widen the scope from those persons, groups and entities placed on updated lists of terrorist groups on formally adopted EU lists (see: Lists) to all those investigated under Articles 1 to 3 of the controversial Framework Decision on combating terrorism (2002) which, despite some amendment, is still ambiguous as to where the line is drawn between terrorism and, for example, large-scale protests. It covers those acting with the aim of:

> *"unduly compelling a Government or international organisation to perform or abstain from performing any act" (Art 1.ii)*

To broaden the scope of cooperation on terrorism to this much broader definition might open the way for abuse and its application to non-terrorist offences.

17 November 2004

Intelligence-gathering Through "SitCen"

In June 2004 Javier Solana, the EU High Representative for defence and foreign policy, announced that internal security services (eg: MI5 in the UK) are to provide intelligence on terrorism to the Joint Situation Centre (SitCen)—part of the EU's emerging military structure. At the same time he revealed that the external intelligence agencies (eg: MI6 and GCHQ in the UK) had been cooperating with SitCen since "early 2002". These moves were clearly needed as attempts to bring together meaningful intelligence on terrorism through Europol were doomed to fail—internal security and external intelligence agencies are loath to share information with police agencies. However sensible this initiative may be it still begs the question of accountability and scrutiny. It would be almost inconceivable at the national level for a body whose role was military to have its remit extended "at a stroke" to include anti-terrorism without a formal procedure being undertaken—and to ensure that a chain of accountability and scrutiny both to government and parliament was set out.

SitCen's job is to produce assessment reports on "the terrorist threat (internal and external)" but it is also to provide reports that cover:

> *"the broad range of internal security and survey the fields of activity of services in the areas of intelligence, security, investigation, border surveillance and crisis management"* (Dutch Presidency Note to the Informal Meeting of the JHA Council in October, unpublished doc no: 12685/04)

The overall concept has, however, swiftly shifted from dealing solely with "anti-terrorism" to "internal security" which embraces all the agencies of the state from the military to the host of agencies who maintain "law and order", from biometric passports to border controls. It is the same in the draft "Hague Programme" on justice and home affairs (the successor to the "Tampere programme"), which refers to internal security as covering: "*national security and public order*."

SitCen will send "advisory reports" to the Justice and Home Affairs Council, reporting "any necessary action", and will cooperate with a host of JHA bodies, including the Strategic Committee on Immigration and Frontiers and Asylum (SCIFA) and the Article 36 Committee (CATS, senior national interior ministry officials), and representatives from the Commission, Europol, Eurojust, the European Border Agency (EBA), the Police Chiefs' Task Force, the Counter Terrorism Group (CTG) and a new "internal crisis management" working party. The EU Police Chiefs operational Task Force, which was set-up in 1999, still has no legal basis for its activities, it is unacceptable that there should be any extension of this group's mandate or remit until this issue is resolved

Under the EU Constitution, SitCen will also report to an "Internal Security Committee" (Article III-261) which will deal with "operational cooperation on internal security". An *ad hoc* "Internal Security Committee", comprised of the chairpersons of the JHA bodies above, is to be set-up in the near future, before the Constitution comes into force. Under Article III-261, the European and national parliaments will only be kept "informed" of the new committee's activities—which on past experience will be bland, general reports. There is no guarantee that documents from this Committee will be accessible and little prospect of the interim, ad hoc Committee being accountable.

The European Border Agency

The EU Border Police is developing in an ad hoc fashion. Before the Regulation establishing an EU Border Management Agency had even been agreed the EU had established a Common Unit of senior border police, operational centres on sea, land and air borders, and a risk analysis centre. Now, before the Regulation has even entered into force (1 May 2005), a broad expansion of the agencies remit and powers is planned. First, through the creation of a "rapid reaction force of experts" available to "temporarily" increase "external border control capacity" (including "intercepting and rescuing illegal immigrants at sea"). Second, through the creation of a "common European border police corps". Third, consideration of whether it should assume wider roles for "security, customs" as well as: the management of large information systems (such as Eurodac, VIS and SIS II) (Dutch Presidency Note to the Informal Meeting of the JHA Council in October, unpublished doc no: 12714/04)

17 November 2004

Data Exchange

Q: *The Commission calls for the establishment of the principle of equivalent access to data by national law enforcement authorities in the EU. To what extent would this challenge fundamental legal and constitutional principles of Member States?*

This proposal is present in COM (2004) 429 and has been widely criticised. It proposes a free, open, market for criminal data and intelligence held by the hundreds of law enforcement agencies in the EU—an idea unlikely to find favour with governments or the agencies themselves (see, Home Office EM, 6 July 2004).

Inside sources say that this proposal is unlikely to survive in this form and that a proposal based on specific requests (on named individuals or groups) is likely to replace it (see for example, COM (2004) 664 on the exchange of information extracted from the criminal record).

The "Hague Programme" speaks in general terms of the "availability" of investigative information from 2008.

Q: *The Commission calls for the interoperability of EU databases. What are the implications of a facility for transferring data between databases? Is there a case for a centralised EU database for all law enforcement purposes?*

The EU uses the term to mean that the various EU databases can be linked or accessed by all law enforcement agencies (the Hague programme refers to SIS, VIS and Eurodac).

The fundamental assumption in the 1990 Schengen Convention is that only those agencies which input data should have access to data in their field. For example, data put onto the SIS by immigration officials would be accessible by them for the purpose of excluding those not to be granted entry.

The change came to a head, after 11 September 2001, when internal security agencies (like MI5) wanted access to all SIS databases. The problem was that such agencies could not abide by the data protection provisions of Schengen. In some states internal security agencies simply submitted searches via police agencies. The solution was "interoperability", namely that a database created for one purpose could be accessible and used for other purposes.

Data protection rights for data held on the SIS are almost unworkable at the moment. Only in a few cases have individuals learnt that action taken against was based on information derived from the SIS. Complaints then have to be made not against the SIS but the state which placed the information on the SIS. Even if erroneous information is deleted by that state there is little chance of tracing and eliminating the "paper-trail" whereby other states have used the information on their national databases.

Any links between Eurodac and other databases should be strictly limited to searches relating to the question of which Member State is responsible for considering an asylum-seeker's application. This would mean that an asylum-seeker's fingerprint sent to Eurodac could be checked against the fingerprints in the VIS of persons who have been issued visas, because that is one of the criteria for allocating asylum responsibility, but not against the fingerprints of persons who have requested visas or whose applications have been refused. Even in the first case a Eurodac/VIS link would have to be denied for the UK, since we have opted out of participation in the VIS and should not be permitted to participate through the back door.

A Eurodac/SIS link should be totally out of the question even when fingerprints are held in the SIS, because the categories of data in the SIS are not comparable to the grounds for allocation of responsibility for asylum applications. In particular it is not relevant for allocating responsibility that a person is listed in the Article 96 category as a person to be denied admission. Nor should it be possible to have links to this data (or other SIS categories) for the purposes of deciding on the asylum application on the merits, since a prior decision that a person should be refused entry to a Member State should clearly not be relevant to deciding whether a person has a valid claim to be a refugee or in need of other protection. Given the weak procedural rights for individuals in relation to the SIS, this would weaken procedural protection for asylum applicants to an even more unacceptable level.

As to the idea of a "*a centralised EU database for all law enforcement purposes"* it can be argued that the SIS in the form of SIS II is developing in this direction. However, it is not intended to cover criminal records which would require "harmonisation" through a standard European Criminal Record—which is many years away.

DATA PROTECTION

Q: *Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the Third Pillar, as advocated by the Commission?*

The question makes an assumption in asking whether "*current data protection arrangements continue to provide an adequate level of protection for the individual*". In our view the current arrangements offer little protection at the moment—this is true of data protection in general (see the Commission's first and so far only review of the 1995 Directive) and certainly as regards the third pillar. The planned functionalities of SIS II and "interoperablility" make the prospect of protection and rights look even less likely than under the present quite unacceptable situation.

What is intriguing about the final version of COM (2004) 429 on "enhancing access to information by law enforcement agencies" is that the draft discussed by the full Commission in May also included the phrase:

"and related Data Protection issues"

And equally intriguing is Chapter III of COM 429 which refers to data protection but in the sense of preparing a Framework Decision:

"in order to empower access to all relevant law enforcement data by police and judicial authorities"

There is no mention of a measure on data protection and the third pillar in the "Hague Programme". The hope for a legal framework covering the third pillar may, it seems, have to wait until the Constitution enters into force and the commitment for data protection covering all EU activities is put into practice.

Footnote:

The issue of data protection in the "third pillar" (justice and home affairs: policing, immigration and asylum and judicial cooperation) has long been recognised as a "gap" in EU policy (the 1995 Directive on data protection does not cover this area). The issue of data protection in the "third pillar" was first raised in the Council of the European Union (the 15 governments) in May 1998. The German Presidency of the European Union, 8 June 1998, said "search for the (lowest) common denominator in this field is not new". However, the "Action Plan of the Council and the Commission on how best to implement the provisions of Amsterdam establishing an area of freedom, security and justice" (13844/98) said that data protection issues in the "third pillar" should be: "developed with a two year period" (IV.47(a)). It was not until August 2000 that a draft Resolution was drawn up by the Working Party—this was revised five times, the last being on 12 April 2001 under the Swedish Presidency of the EU (**6316/2/01**) when agreement appeared to have been reached—and the Article 36 Committee was asked to address outstanding reservations. This draft, although peppered with exceptions and derogations, could have been the basis for a public debate. However, since 12 April 2001 there has been silence—and under a rationalisation of the Council's working parties from 1 July 2002 (**6582/1/02 REV 1**) (reducing the number of Working Parties from 26 to 15) the Council's Working Party on data protection was abolished without explanation.

Immigration and asylum legislation now makes reference to the data protection directive—however, the Commission has long being saying that it plans to set out standard rules on third pillar data protection, but has never done so.

Q: *Should there be common standards for the transfer of personal data from EU bodies and the Member States to third countries/bodies, including Interpol?*

Yes there should be but it depends on the "common standards". Europol is now authorised to exchange personal data with a host of countries and agencies. This authorisation based on reports on data protection from the intended third states—these are uniformly based on the "legal position" and not on the practice.

"Common standards" have to be based on the fundamental principles of the 1995 Directive, the 1981 Council of Europe Convention and recommendation on policing data, Article 8 ECHR, relevant case law of the European Court of Human Rights, along with the specific right to data protection set out in the EU Charter of Fundamental Rights.

Such standards would, for example, have ruled out the EU-USA agreement on PNR (passenger name records). The USA does not have a data protection law covering EU citizens and has the clear intention of using the data for purposes other than for which it was collected.

17 November 2004

The Role of the EU

Q: *Is there a need for an EU intelligence policy, as advocated by the Commission? To what extent can EU objectives be identified separate from those of the Member States?*

This question should perhaps be more specifically defined. We presume it refers to an intelligence role in relation to terrorism and not a general intelligence role.

There is a clear and legitimate role for the EU to have an intelligence-gathering capacity in order to combat terrorism. However, any extension of this role to cover "any threats" (as we have seen in a recent Council document) would raise major questions of accountability and decision-making (see the answer to the first question).

Q: *How important is it for the EU to speak with one voice in the international arena in matters involving counter-terrorism co-operation?*

This is hard to envisage. Firstly, there is the special relationship between the UK and the USA dating from 1947 (UKUSA agreement) and their sharing and gathering of intelligence through GCHQ and Echelon. Second, many major policy initiatives are formulated in G8 (and its working parties).

We believe that there is another major issue which needs to be addressed in this context, namely the growing influence of the USA over EU justice and home affairs policy-making. During each six-monthly Presidency cycle there are at least 40 high-level meetings (some by video-conferencing) on JHA issues.

These meetings are not simply exchanging views or ensuring operational cooperation but are leading to issues of "concern" to the USA being placed high on the EU agenda (eg: preparatory offences related to terrorism). We will be happy to elaborate on this aspect orally.

Q: *The United Kingdom recently hosted a summit of five Member States ("G5") to examine measures to combat terrorism. Do moves of this kind prejudice EU wide initiatives?*

It is interesting to note that membership of the "G5" group set up last year—UK, Germany, France, Italy and Spain—overlaps with EU membership of G8—UK, Germany, France and Italy (with the exception of Spain, then under Aznar).

G5 because it is not subject to any form of accountability or public or democratic scrutiny and appears to be having a growing role in driving the JHA agenda. It does not meet the criteria for enhanced co–operation since it does not follow the obligation to apply EC or EU processes (which would entail some degree of accountability and scrutiny) and it does not meet the criteria for minimum participation by Member States (at least 8). Why should the large and powerful interior ministries of these member states be able to dictate to the Commission, the European Parliament, national parliaments and smaller member states.

Institutional Arrangements

Q: *What is the added value of the post of EU Counter-terrorism Co-ordinator? What should his role be?*

The value of having a Coordinator is perhaps not so much the post itself but an indication that there is an intention to coordinate the different initiatives in a way that was clearly not the case before 11 March 2004 (Madrid)—three days prior Mr Solana had produced a lengthy report on the many shortcomings in anti-terrorist planning, coordination and operations.

Q: *What changes are called for in the EU's institutional arrangements (including Eurojust, Europol, the Chief Police Officers' Task Force, and the Terrorism Working Group) in order to combat terrorism more effectively?*

The current plans, and the creation of the Article 261 Committee under the Constitution, should provide the means necessary to combat terrorism. The problems will arise if the Article 261 Committee and SitCen take upon themselves—as there is a clear intention to—a wider role. This is to say all the ramifications of "internal security" as distinct from counter-terrorism.

17 November 2004

The Article 261 Committee on operational cooperation on internal security presents its own problems of accountability. European and national parliaments are only to be kept informed of it's activities and whether the Regulation on access to EU documents will apply to it or whether a standard exception under Article 4.1.a will be routinely used is not clear.

Tony Bunyan, Steve Peers and Ben Hayes

12 November 2004

Examination of Witnesses

Witnesses: MR TONY BUNYAN, Chief Editor and MR BEN HAYES, Statewatch, examined.

Q295 ***Chairman:*** Welcome again to two old friends of this Sub-Committee, Tony Bunyan and Ben Hayes from Statewatch who last gave us evidence in our Europol inquiry, I think. We are very grateful to see you again and we read with great interest the papers that you have put out. I would like to thank you on behalf of the Sub-Committee for the paper that you sent us, which made very interesting reading. I will not repeat what I said earlier about the subject of the inquiry because I have already stated that. We have registered relevant interests and I understand you have had a copy of those. I wonder if you would like to make an opening statement before we launch into questions. Would you like to do that, Mr Bunyan?
Mr Bunyan: I think it may be addressing the general question: has the response to 11 September and then Madrid been a response which has led to some concern that it is going farther than tackling terrorism? Ben is going to talk in a second, but I think this has been our concern since 11 September when we first of all saw the draft decision on how to define terrorism. It was as a result of some work by civil society in that very difficult atmosphere of the autumn of 2001 which managed to get some limitations on that definition of terrorism so that it was made clearer—although not totally clear—that it did not refer to normal democratic activity; it did not refer to trade union activity. That was a difficult time to do that, to be raising those issues. Similarly on 25 March when there was a special summit and we produced a scoreboard—which Ben was very instrumental in doing—which showed again great concerns about how many of these measures were directed at terrorism and how many were to do with crime in general or surveillance in general. A classic issue would be data retention or biometric passports and to what extent are those both necessary to combat terrorism as distinct from combating crime in general. Perhaps I could ask Ben to talk a little bit more about the conclusions we came to in the scoreboard after 11 March.
Mr Hayes: It seems to me the best way to answer the question of whether the terrorism proposals are proportionate and justified is to look exactly at the content of the EU action plan on terrorism which was adopted just a fortnight after the terrorist attacks in Madrid. What the Member States did then was to endorse 57 separate proposals. A number of these proposals could potentially introduce wholesale surveillance of everybody in Europe through telephone communications, the so-called data retention proposal, tracking all air travel in and out of the EU and creating records on air travellers (the so called PNR scheme) and the fingerprinting of nearly everybody in the EU, the three separate biometrics proposals. Tony has already made the point of whether this is a justified anti-terrorism measure or measures, or whether this goes further. There is also a question of whether the EU is actually exceeding its mandate as it certainly appears to be with the biometric passport proposals. This was apparently expressly ruled out in the EC treaties. The second issue is the fact that of the 57 proposals it is our view that at least 27 of those have very little to do with combating terrorism per se; they are about surveillance, they are about combating organised crime. It seems that what has happened is that the EU just took much of the Justice and Home Affairs agenda for policing and judicial co-operation and moved it across under the banner of anti-terrorism. There is a question there of not only whether this is justified, but whether it is even cynical because some of these proposals are so unrelated to terrorism. Our position has always been that what is needed is good, intelligence on specific threats not mass surveillance of everybody which is going to generate more data than can possibly be usefully analysed.
Chairman: You have very neatly and very succinctly answered my first two questions so I will move smartly on.

Q296 ***Lord Dubs:*** Could I possibly ask a supplementary? You expressed your concerns about fingerprinting and biometric data and so on; would you have fewer concerns if you were satisfied as to the safeguards regarding the use of such information?
Mr Hayes: We would have few reservations about the use of a technology that was able to prove that an individual is the individual that they say they are through the use of their document. What the EU is talking about doing is creating either an EU passport register or a register of all travel documents, which is

also going to include resident permits and all visas, and then making this database—whatever it is they create—accessible to law enforcement authorities for general law enforcement purposes. That is where our great reservations come into this. It seems that it is not just about individual documents, security and identity—being able to prove that an individual is who they say they are—but about creating a central database that will in effect cover the majority of the EU's population. We have grave reservations there.

Q297 ***Lord Dubs:*** Does that not depend on how that central database is used or are you concerned about the fact of it?

Mr Bunyan: If we take the position of the Article 29 Working Party which is a Working Party of all the data protection commissioners, when they looked at it they said they have no problem with, if you like, "one-to-one" identification. I mean, "Are you Alf Dubs walking into the building?" "Yes, you are. You have a card which says you are, that is checked." They have no problem with that being localised in terms of a company or the Home Office or wherever; that somebody going into that building is a person entitled to go into that building. Their problem arises when you are doing "one-to-many" checks, when you have centralised databases. The case we are talking about is where national information is not only kept nationally but is also kept on an EU database and then accessible to many, many organisations. I think one does have to have some very big concerns about going to that system where you are putting it on an EU database. Secondly, you have to have concerns that data protection in the EU just does not work. Nobody actually knows how to protest if they think they are on the Schengen Information System. We know of instances where people have got onto the Schengen Information System and it has taken them years to get off it when they were not meant to be on it in the first place. I think there is a real problem initially and I think there is a problem about whether you can actually guarantee any protection for people who are wrongly on the list or their information is wrongly used or wrongly added to.

Q298 ***Baroness Gibson of Market Rasen:*** That actually answers one of the questions I was going to ask you, but I will go back to the Commission and the terminology being used. The Commission refers to the principle of "equivalent access" to police data, while the Hague Programme talks about the principle of "availability". I wonder what you feel about this terminology and whether it does actually represent different approaches.

Mr Bunyan: I have found myself incredibly confused by the different communications coming out. These communications have been coming out of the Commission and they seem to be written by the same group or possibly the same person and there is one about the exchange of data on terrorism, there is one about the general exchange of data and then there is a third one on creating a European criminal record. They all use the same sort of logic that somehow there is a continuum of activity—between terrorism on the one hand, serious crime and, indeed, everyday crime. To answer the specific point, what has happened is that COM 429, which is the one on a free market in law enforcement information, whereby in theory any agency in Britain could have access to a database of an agency in Austria or Latvia or anywhere else, quite frankly is not going to happen. It is not going to happen because nearly every Member State—including our own—is not happy with people coming in and looking at their databases. Obviously as civil libertarians we are concerned about it, but on this issue I think it is unlikely to happen. What is much more likely to happen is the principle of availability. This is what COM 664 is talking about but in a very limited sense on convictions, so that the question would be: "will you provide information on this particular person or will you provide information on a person who is in a Member State of the EU and convicted, will you pass that information over?" Say someone is convicted here but is Italian; will you pass the information on their conviction to the Italian authority? One can have little objection to that because we are not talking about intelligence here, we are talking about somebody having been charged, convicted and sentenced and that information being passed from a UK court to an Italian database. That is understandable. We have no problem with that area. However, there has been a confusion. I think the initial paper was talking about the sharing of all the information on everything and, as we have said in our paper, we are extremely concerned about something which is going ahead at the moment—the sharing of information during investigation of terrorist activities. We are extremely concerned about this and about who could get caught up in that net. We have used the example of the ten Muslim men who were arrested in Manchester who were then released without charge. I have looked at the work of intelligence agencies over the last 20 or 30 years now. If one individual is being investigated the whole of their social network and friends and people at work are investigated. The idea is that all that data could or should be passed to all the other agencies in the European Union of which there are several hundred, but there is no obligation to take information off. One only has to think of the classic case of Senator Ted Kennedy who was arrested five times in a row because he happened to have the same name as someone who was on one of their watch lists. He had to get in touch with the head of Homeland Security in the United States to be allowed on a flight

back to his home state of Massachusetts. If you start to get the building up of people onto watch lists—which we are beginning to see both in the United States and the European Union—then I think there is a real concern. All one has to have in this particular case is a proviso that of course it is legitimate in the course of investigation, that you should pass it over very quickly in case there is some evidence from another EU state, but there should also be an absolute obligation that that information is deleted if that person is not charged with any offence.

Mr Hayes: I think maybe there is a second issue here as well. If you look back through the history of EU justice and home affairs co-operation, you have had the Schengen Convention—now incorporated—the Europol Convention, the Mutual Legal Assistance Convention and a host of joint actions and resolutions that all provide for spontaneous data exchange not just in relation to terrorism but any serious crime. Suddenly, since September 11 and March 11 they have just said that they need a host of more measures. There has been no idea of reviewing the systems already in place to see if they are working properly and to find out whether we actually need all these new systems. It just seems to be racing ahead of itself without any kind of question of looking at whether the things we have work properly already. Perhaps it would be better to go back to things they spent years drawing up for precisely these kinds of situations rather than just going full steam ahead into something else.

Q299 ***Lord Dubs:*** The Commission's most recent proposals envisage access by law enforcement authorities to the databases of financial institutions. Do you have any concerns about that?

Mr Hayes: There has traditionally been a big problem with banking secrecy hindering investigations so there is clearly a need to do something about that. It is not an area I know a great deal about, but as I understand it we already have a system for flagging up what are called suspicious financial transactions. Most countries have those but the amount varies; I think here it is £2500. We then also have a network of financial intelligence units that have come out of both EU measures and the OECD financial action task force. I am not fully up to speed with the Commission's proposals, but where it seems they might be going is just to give direct access to law enforcement to these databases. That then raises the question of how are they going to use that access? Are they just going to go in for what we call fishing expeditions and what are the implications of that to the warrant system? At present in any terrorist investigation it is extremely unlikely that any warrant to turn over this kind of data is going to be refused. Are we moving—with all this direct access to these databases—away from a system of warrants? You cannot ask for a warrant for lawful interception or access to data in relation to persons unknown for crimes unknown, and I think there is a real question of how are you going to ensure adequate judicial oversight of access to these databases by law enforcement and what kind of audit trail is there going to be in the event that data is used unlawfully or exchanged illegally. That would be our concern there. As I say, I am not fully up to speed with what the Commission is proposing; it is one of the most complicated documents I have ever seen.

Chairman: Can we move on to the data protection area now and I know Lord Avebury would like to ask a few questions.

Q300 ***Lord Avebury:*** You have already said that existing data protection arrangements applying to the Third Pillar are grossly inadequate and you have given the example that a person cannot readily correct errors or have data expunged when it is no longer required. Are there any other aspects of the data protection arrangements in the Third Pillar that you think should be strengthened and would it be satisfactory simply to transfer across the arrangements that already exist in the First Pillar?

Mr Bunyan: Let us deal with the 1995 Data Protection Directive which we have adopted in this country and it has been adopted by the EU. It took the Commission five years to produce their first evaluation and what is striking about that evaluation is the fact that there is a great variety between Member States as to the powers given to the data protection authorities, to the staff they have and the resources they have. Without a shadow of a doubt the system in some of the German Länder is the strongest. They have good staff; they have the power to walk into any police station at any time; they can examine records. When we compare it to our system here, we can say that Richard Thomas is doing a good job but lacks the same powers that they have, for example, and lacks the resources. In a sense one could say that the Information Commissioner is able to keep up a general role and keep the thing going down a broad road, but even he is concerned about where we are going—whether we are "sleep walking into a surveillance society". The truth is that the degree of control varies too greatly. The Commission recognises this, not that it has produced any measure since it produced its report last year, nor has the Council said that perhaps we should be harmonising, we should have some common standard across the EU about what minimum standards of staffing and powers. Even then the problem with that is that it does not cover the Third Pillar; it does not cover the issues we are really talking about—policing and immigration records and terrorism. There has been a lamentable lack of political will in the Commission and by the Member States and by the Council to

produce a data protection measure covering the Third Pillar. In our note we say that they started to look into this in 1997 and then abandoned it in the spring of 2001. We happened to apply to the Commission for a document to get this further information. At the time the Commission proposal on exchanging data did have tagged onto it, as discussed in the full Commission, "related data protection matters". But when you look at what they mean by "related data protection matters" it actually means freedom of information for the law enforcement agencies. It is not about data protection for the citizen. The real fear in this area is that there are so many measures being put in place since September 2001 and certainly since March 11 that before we get round to data protection in the Third Pillar the States and all the agencies will have all the powers they want and therefore the kind of measure you can get into force will be circumscribed. One might add that the same goes for the whole of criminal justice co-operation because the rights of the defendant still are not defined and yet we have many EU-wide powers and the last thing apparently on this road is to define the rights of the defendant. There is a parallel there. It seems to be completely wrong that we should be giving powers to agencies in the collection of information without in parallel and at the same time having a real balance between civil liberties and security rather than putting more security measures in place and then getting round to aspects of personal data protection.

Q301 ***Lord Avebury:*** Can I take it then that you do not actually consider that if we were to apply the legal framework that exists for the First Pillar to the Third Pillar that that would necessarily grant adequate data protection?
Mr Bunyan: No.

Q302 ***Lord Avebury:*** Is it possible that you could not immediately in an answer to me but perhaps let us have a note of the respects in which you think First Pillar legal provisions would be inadequate if they were simply transferred across to the Third Pillar.
Mr Bunyan: Of course.

Q303 ***Lord Avebury:*** Thank you. Do you think that there is a need for the development of specific legal rules to regulate the exchange of data between police authorities in the EU? Could you say what principles they should contain, either now or in the note that you are going to let us have?
Mr Bunyan: We could do that in a note as well; I think the two are connected. In very broad terms we do not think there should be general access to all data held only specific data. Quite frankly, the powers exist for that at the moment. As Ben has pointed out, we would be doing well to actually look at some of the powers which have not even been exercised yet. There are some areas where they do not have in the European Union or in other national parliaments this kind of scrutiny committee which is not just looking at things before they are adopted but actually can look back at them after they are adopted. This is a uniquely UK phenomenon which we often urge on the European Parliament Committee. There are so many new measures and they have no time at all to look back at what has been passed and to scrutinise how is the law being used, is it being properly, does it need more backing? I think there are a number of issues here which we could perhaps take up.
Chairman: Can I just make a brief correction because I do not think there are many police authorities which would oversee the work of what the police are doing in the EU, so it is police forces we are talking about rather than police authorities.

Q304 ***Lord Avebury:*** You mentioned some cases of serious misuse of personal data. You gave us the instance of the people who were connected with the arrest of the Muslims in Yorkshire. Could you give us any other examples of misuse of personal data, particularly in relation to exchanges of data between European countries?
Mr Bunyan: The famous case is that of the brothers, the Welsh football supporters, who happened to go to a football match. They travelled through Belgium and then Luxembourg and then they were arrested. They were chucked out and found themselves on the Luxembourg records, on the Belgian records, on the UK Foreign Office list and on the NCIS list in London. It took them five years because what they had to do was not only get off the list in Luxembourg, they then had to get off the NCIS list, then they had to get off the Foreign Office list and then they finally had to get off the Belgian list. The European Commission had to be involved to order the Belgian authorities to take their names off the list. They had actually never done anything wrong and when they went back a second time one of the brothers was handcuffed and sent home from Belgium, in handcuffs, on the Harwich ferry. What it did tell you is how difficult it was to get your name off a list. We do know for a fact that there are several hundred—probably over 2500 people—who have been stopped at borders after what happened in Genoa in the summer of 2001 who have been told: "you are not being allowed into Italy, you are not coming into France, you are not coming into Spain because you are on the Schengen Information System list". For those people to try to discover who put them on the list and how many countries' lists they are on is a nightmare. We have helped one or two people but we are not unfortunately a group who can spend time doing that, we are mainly a research group. It is really difficult for people.

Q305 ***Lord Avebury:*** But there is no European group which maintains a record of all these individual cases such as the one you mentioned.
Mr Bunyan: Unfortunately not. It is very difficult if you are just turned back at the border because there is nothing written. You appear at the border and are told you cannot enter a country because you are on the Schengen Information System and you are a threat to public order. They will not let you through. It is incredibly difficult for people. I think the European Court of Justice is actually looking at a case of people going to Spain which included MEPs—and because they were MEPs it has got a slightly higher profile. This case is the refusal of the Spanish authorities to let a group enter Spain for a conference in Barcelona. We are waiting to hear what the European Court of Justice is going to say, but for the ordinary person it difficult to find anything out.
Mr Hayes: The main problem with all these databases is that the rules and procedures for adding people are so vaguely defined that what you get is essentially a political decision. What France did as a result of the activities of Rainbow Warrior, the Greenpeace ship, was just to register wholesale a number of Greenpeace protesters, as a response to the political activities they had been doing. One famous case was Stephanie Mills from New Zealand who was a Greenpeace protester. She had never been charged with any public order offence but when she arrived at Schiphol Airport in Amsterdam she was refused access to the entire Schengen territory. You asked for an example of serious misuse of personal data, the PNR scheme, which I am sure you are all aware of, and the treaty between the EU and the United States to allow the exchange of information on passengers is, I think, another perfect example. If you want to book a flight on British Airways and go to, say, Aberdeen or Genoa you click through the booking process and you have to tick the little box to say that you understand BA's privacy policy and if you do not tick that box you cannot proceed with your booking. If you look behind that box what it actually says is that you theoretically have a right to data protection—I do not know whether it refers explicitly to the treaty—but we are going to be sharing your data with the United States. You are not even flying to the United States; the problem is that you are flying on a carrier that flies to the United States and the only way to implement the PNR treaty was to give the US direct access to the EU reservation databases. If I say, actually I am not happy because I am only flying to Genoa and my data is potentially going to be handed over to the Department of Homeland Security and shared across this myriad of agencies in the US, I cannot proceed with my booking.

Q306 ***Lord Avebury:*** I think you have indirectly answered my next question which is: should the European Union develop common policy for the transfer of data to third countries and organisations? If so, what should the main principles of such a policy be?
Mr Bunyan: I went to a hearing in the European Parliament on this issue of PNR data protection and I produced four different versions of data protection in terms of the EU acting externally. They had the one on the table for the United States; they had another one for the exchange of information with police forces; and there was another one that Europol had in two different versions. It is not working properly across the EU but the 1995 Directive is a very good basis to start from if it were properly enforced and properly serviced. However, it cannot mean anything because the minute we go outside the European Union to negotiate with Russia, for example, to meet their needs we somehow unscramble it; some countries do not have any protection laws themselves. There is a real problem here. I think that the computer reservation system is covered by a regulation; not a directive, a regulation. The Commission has it in its power to order the computer reservation systems not to give any information to the United States until they have met the provisions of the EU statutes. But then politics comes into it. The Commission said: "We know we have that power but we dare not exercise it because Member States would not agree with it". My answer to that is quite simple: "I am terrible sorry, but the Commission is the custodian of the law". When it comes down to regulations it should have been doing its job. Then we would not have got into this mess because the airlines would have been told that they cannot give information out until there is an agreement which meets our standards. I am not saying there is not an agreement, but one which would have been much stronger and quite different to the one that was reached if the Commission in this case had used its powers.

Q307 ***Lord Corbett of Castle Vale:*** There appears to be a proliferation of agencies and formal and informal structures in the EU for dealing with counter-terrorism. Is there a need for better co-ordination or streamlining of these bodies? Should they all be brought formally within the EU structures? You have been very critical in your paper about a whole number of these informal arrangements.
Mr Bunyan: I think there are two answers to this. There is an answer in terms of some of the central bodies and there was a report that was alluded to in our note which came out on 8 March—three days before 11 March—which was a highly critical report of what the EU had and had not done on counter-terrorism. It is a very interesting report that is primarily concerned with terrorism and not crime more generally. It includes things like the fact that the

remit for Europol to have a counter-terrorist group had run out the previous summer. It includes the fact that two of the three working parties on terrorism were capitals-based rather than Brussels-based. That means that instead of meeting in Brussels with a Council Secretariat servicing them, one was meeting in Berlin and one was meeting in London. In other words, the membership of the three working parties on terrorism were not talking to each other and were being serviced in each case by different secretariats. We can see the need quite clearly for that to be put right. One of the things we are seeing from conclusions coming up at the next Summit is that that kind of nonsense is going to be sorted. Our argument throughout is that legitimate anti-terrorist measures we will back to the hilt. There are other areas where one does have concern. One has concerns about the Police Chiefs Task Force. We have a document—which we are not meant to have—on the so-called positioning of this Task Force, which is dated three days ago and shows that they are still trying to find a place to put it to give it a legitimacy, a legal status, and yet this is a meeting of the now 25 senior police officers dealing with operational matters and planning matters, a group which even wrote its own remit and gave it to the Article 36 Committee, which endorsed it. You have police officers writing their own remit, going to their bosses who rubber-stamp it and yet it has no legal status within the European Union. That worries me. It worries me when this Committee—or I think it might have been Sub-Committee E actually—spent quite some time looking at the creation of ad hoc multi-national teams in the European Union, which we are still extremely worried about. This is the idea that not all the EU Member States take part but you could have France, Italy and Spain if we decide to have a multi-national team which has nothing to do with arresting people but is there to undermine and keep under surveillance suspected terrorist groups. We read this, as did the Select Committee as a whole, and were highly critical. If they are terrorists they are terrorists and you should be arresting them. Where are we going? Is this is going to be like the Force Research Unit in Northern Ireland which started off as a research unit and ended up assassinating people. It did happen for over 20 years in Northern Ireland. There are elements at the edges and in the ad hoc area where one is frankly really quite worried about, first, accountability and, secondly, what might be happening on the streets. At the central level, then we support the kind of co-ordination that is going on. I hope I have not confused you, but there is a difference in the two approaches.

Q308 ***Lord Corbett of Castle Vale:*** Not at all; you have more than half answered the next question I was going to ask you, which is fine. You are very critical across the board in your paper and in what you have both said this morning on grounds of accountability, transparency and human rights. I think the accountability and the transparency are obvious. What are the human rights dangers in this apart from the data protection area, which we have been over?
Mr Hayes: In respect of the development of these EU bodies there are so many different measures that I think you have to take each specific measure and ask what concerns does that raise. When you are talking about EU bodies you are also talking about the databases. We have all these plans for the second generation Schengen Information System. If you are going to have people subject to what are effectively law enforcement sanctions—i.e. you are not allowed to travel and things like that—you are going to raise broader human rights questions: fair trial, procedural rights, safeguards and guarantees. I think the problem again is that basically human rights are an add-on in EU decision making; they are not being put in centrally and saying, "Here is the Human Convention, here are the human rights, these have to be safeguarded in all the measures that we do". What you are seeing are measures that contradict human rights and then people coming back to the EU and saying that these measures are a problem. Tony referred earlier to the Framework Decision on the procedural rights and guarantees for suspects and defendants: we have had the whole mutual recognition programme, which was supposed to be a twin-track programme about judicial cooperation on the one hand and the protection of suspects' rights and defendants on the other. There are 25 measures to do with facilitated judicial co-operation and nothing to do with procedural guarantees. It dovetails with the question of data protection. The problem is that there is no body in the EU pushing human rights and data protection accountability as a whole. There is no human rights commission; there is no human rights working party within the Third Pillar. There is just law enforcement. You can take any measure you like across the counter-terrorism spectrum and you are running into the same problem.

Q309 ***Lord Corbett of Castle Vale:*** Given that the role changed on 11 September both in the scale and barbarity of that act of terrorism, is there not inevitably a compromise which has to be made somewhere? You can argue about how far it should go and the rest of it, but where people can prove both necessity and appropriateness there are going to be occasions in these areas of accountability, transparency and human rights where a compromise actually has to be made if you are going to be able to reassure your citizens that you are doing all you can to safeguard them from terrorist attack.

Mr Bunyan: That is a very difficult area. If you take the EU after 11 March, when that happened of course people in the Council and the Commission were suddenly asked by the politicians, "Give us a list of things we can do". This is the difficulty. At some stage there needs to be somebody sitting down and taking a perspective, even at that difficult moment. There was just the Commission, scrabbling around to find things out of the FB6 research programme.

Q310 ***Lord Corbett of Castle Vale:*** You cannot know that nobody considered these issues alongside the other things that were going on. It may not have resulted in what you wanted, but are you saying they were just scrabbling round. I think you used that phrase?
Mr Bunyan: Yes, I used the term scrabbling around and I use it particularly in the case of this COM 221 and 429. They were ideas which came out very quickly in a pre-25 March paper from the Commission, were grabbed by the Council to put into their Action Plan, where they are now. At least in one case—the use of biometrics—we have been highly critical of these ideas (as have other people) in terms of where this information is going. In that moment in time it does need mature, political hands-on judgment saying: "Hang about a minute, what has biometric passports got to do with terrorism?"

Q311 ***Lord Corbett of Castle Vale:*** You say it has nothing to do with terrorism.
Mr Bunyan: I am saying it has very little to do with terrorism, yes.

Q312 ***Lord Corbett of Castle Vale:*** Is it not the most effective way we know at the moment in establishing identities?
Mr Bunyan: No, it is the least useful way. Perhaps I should explain why. Anybody who is in intelligence or security will tell you that all you are doing is building a bigger and bigger haystack to find the same number of needles. In other words, everybody becomes a suspect.

Q313 ***Lord Corbett of Castle Vale:*** I know that argument, but technically I think you said there is very little assessment from the biometric information on firmly establishing somebody's identity.
Mr Bunyan: I meant in terms of combating terrorism. Identity obviously; fighting terrorism is what I was questioning.
Mr Hayes: At the same time it must be remembered that the September 11 hijackers were travelling on genuine documents. And Spain has long had an identity card system.
Mr Bunyan: Let us assume that we have a passenger name record checking system in the EU within five years: if somebody books and they are on a terrorist list they are presumably going to be arrested when they get to the airport so the known terrorist—the person on the watch list—will not be allowed onto the plane. If, on the other hand, you are not known, you have no criminal record, you have your biometric ID card, you are not a suspect and you are going to get on the plane. The truth is, all these systems are only as good as the intelligence that you have.

Q314 ***Lord Corbett of Castle Vale:*** I do not want to get into a detailed argument about it, but even though there is nothing known about you in terms of charges or convictions, it may be that there is information on you hanging about and someone can then make a connection. Is that possible?
Mr Bunyan: That is possible. You do not have to have a biometric passport in order to do that. That is about checking every passenger against a criminal record database or an intelligence database.

Q315 ***Lord Corbett of Castle Vale:*** No, it is not; it is more than that. That is the point I am making. If there is no criminal record but there is intelligence held by one or more countries but is not known otherwise.
Mr Bunyan: That is another area where you had better have another note about our concerns. We are extremely concerned about the role in all of this of the United States and the whole G8 structure, which, in our view, is where a lot of the major decisions have moved out of the EU and into a G8 working party.
Chairman: It would be very helpful to have a note about that. I know Lord Avebury wants to follow up on that.

Q316 ***Lord Avebury:*** I want to follow up what Mr Hayes was saying about there being no prior scrutiny of compatibility with the Convention when they introduce all these different directives and instruments. Are you, in fact, advocating a system such as we have with our domestic legislation that somebody in the Commission should actually have to write a certificate saying that the provisions of this instrument have been scrutinised and are found to be compatible and we commend them.?
Mr Hayes: It would be an extremely progressive move to introduce some kind of human rights accounting. I am not convinced that the certificate method on its own is actually always going to be based on a genuine audit of a specific measure. If it were just for the Commission to say, "We have checked that proposal against Articles X to Y and it's fine" that would be a step forward but I do not think it would address the problem that I am talking about.
Mr Bunyan: To give an example of how this can work, Europol now has dozens of agreements so that it can exchange data with other countries' police forces. In every single one of the reports the legal

position is described: in other words, what is Britain's Data Protection Act, for example, and how is it meant to work. We sent it to colleagues in Norway and Germany and asked them what they thought of the reports. They said that it was a statement of the theoretical legal position. Nowhere has it been taken into account how does it actually work in practice. All these reports and all this exchange of data internationally is not based on how does data protection work in these countries, it is based on what is their theoretical data protection regime. There is a really big gap there because on this basis you can declare countries like Colombia, Argentina, Chile and a number of other countries as being safe countries now for Europol to exchange data with. Remember what this means: it does not necessarily mean just Europol giving data out, it means that somebody who is put on a list might come onto a new list because they have been signalled or flagged from the kind of intelligence being mentioned by Lord Corbett that they are suspected of something.

Q317 ***Lord Avebury:*** Do you know of any cases which have been brought before the European Court which arise out of actions taken in pursuance of the powers that have been granted by any of these anti-terrorism measures?
Mr Hayes: The main one is the EU terrorist list. A UN Security Council Resolution—I think it was Resolution 13-73—said that all UN states must implement the sanctions regime drawn up by the Taliban Sanctions Committee, which was originally to freeze the assets of people who were suspected if co-operating with the Taliban. After September 11 this was just extended into a broad, general terrorist list that now covers 400-plus groups. In implementing that Security Council Resolution what the EU did was to create a mechanism by which it could draw up its own terrorist list, and there are now 51 groups and individuals inside the EU and 51 groups and individuals outside the EU on that EU list. The problem comes if you happen to find yourself on that list. There is no mechanism for appeal at the national level, neither is there a procedure for appeal at European level. So what you have is something like a dozen cases lodged with the European Court of Human Rights and several lodged with the European Court of Justice to try to get the regulation overturned, although I understand that they were judged inadmissible. Aside from the terrorist list, I am not sure there is anything resulting directly from the EU measures, although there would certainly be cases coming out of national jurisdiction, I should imagine, where people have been unable to get domestic remedies.
Mr Bunyan: Again there is both a formal level and an informal level. On the formal level you have people on the list and we have just put on our website the case of Professor Sison in the Netherlands; his case is up before the Court in Luxembourg today over access to documents. Why is he on the list? He could not get access to documents in his case. At least that is a formal procedure; at least this person—rightly or wrongly—knows he is on the list. All his assets have been frozen. There is a big issue there. There is another problem which again one notices at the informal rather than the formal level: it appears that there is a Member State of the European Union which is using the Schengen Information System to put alerts on that System of the people who are on that list and of people belonging to the organisations on that list. That is unlawful.

Q318 ***Chairman:*** Do you have evidence of this?
Mr Bunyan: Yes.

Q319 ***Baroness Gibson of Market Rasen:*** Is that just within their own country?
Mr Bunyan: There is a Member State which knows it is acting outside the law and it would appear also that other Member States—knowing that this Member State is prepared to take this risk—are sending that Member State names to put on the list because they dare not risk the legal position in their own country. This is where we talk about things being unaccountable: if that kind of thing is happening, that is state agencies running out of control, you cannot have that. We are not saying that we object to people being on a list, but as several of you in this room will know, there are a number of organisations on the list within the European Union which a number of people would dispute whether they should be on that list at all. This means that people thought to be members of those organisations could be put on an alert list either to be not allowed in the European Union or, perhaps more likely, to be kept under surveillance (of course you do not always know that). The flag is not flown when they are first under surveillance but when they move from country to country. You may never know that you have been flagged for surveillance any more than in this country you would know you were being flagged for surveillance by MI5 or Special Branch. You only know if they do something about it. As I say, there really are some areas that we are getting into of serious concern.

Q320 ***Lord Wright of Richmond:*** I would like to pick up two things that you are obviously unhappy about in your note. The first is the role of SitCen and the internal Security Committee envisaged by the draft Constitutional Treaty. Would you like to spell out briefly what your concerns are about that?
Mr Bunyan: The Situation Centre is part of the EU's evolving, developing military structure. It has a military purpose; it is there to provide intelligence to

the EU primarily on military situations or crisis situations around the world. What happened was that we discovered in June when Mr Solana announced it that it was also being used to gather information and assessment from the internal security agencies like MI5 and had been doing so for the external intelligence agencies since the previous year. In writing about that we have said that that is very sensible. It is quite obvious that you are not going to get real intelligence sharing by Europol; that was never, ever going to happen in a million years because intelligence security services will not share—apart from in specific cases—real information with police agencies because they do not trust them. It is a positive thing that this should be done. The problem one has is that there is no mechanism for accountability. It is a bit like saying we have defence intelligence staff over there, the MoD, which we have had for many years, and we want someone to look at the internal intelligence in Britain, why do we not give them that job? At a stroke, as it were, instead we have created MI5 and although it was mysterious for years at least there is some accountability for it, there is some consciousness and limits to its action. In a democracy that is how it should be. The difficulty in the European Union is that this development is happening, as it were, out of sight and out of mind. One is not saying anything against the development, it is a very logical development, but there should be accountability and there should be scrutiny laid down. The other concern is that you suddenly see this new SitCen role is then creeping back into the way the EU wants to run itself under the new Constitution, which they are not waiting for. They are creating an ad hoc committee now but under the Constitution they will have the Article 261 Committee on operational co-operation on internal security. They are already talking in documents about SitCen not just providing briefings on terrorism—which we say is fine—but on border controls and public order. We are seeing slippage; we are seeing function creep. Some people may say that they do not mind seeing that function creep and all I would say to that is fine, make the argument for it but make it accountable. Do not let us have this function creep. By the way, when you look at the Constitution there is no guarantee that this committee is going to meet in public or have minutes published or we will even have access to documents. You will be pleased to know that the national parliaments and the European Parliament are to be kept informed. I have sat in this Parliament, I have sat in the European Parliament and being kept informed means that you get the most bland report and you have no control or accountability whatsoever. They have come to a situation for the exchange of documents, for example, in the Foreign Affairs Committee in the European Parliament whereby we can get access to certain documents. There is the beginnings there of some kind of parliamentary accountability in the area of Foreign Affairs. There is a way round this which does not endanger the legitimate monitoring of terrorism.

Q321 ***Lord Wright of Richmond:*** I want to pick up your objections to the G5 grouping. I think you have already answered this in talking about ad hoc multi-lateral groups. Is it not reasonable and perhaps inevitable that in a Union of 25 members in terms of practicality you should have smaller groups looking at matters of common concern? Perhaps I should ask you—throwing back the word at you—is your objection theoretical or practical?
Mr Bunyan: It is practical. I must admit now increasingly I am finding with this question of the 25 Member States, what is the problem? We are getting QMV everywhere now. We are going to have it from next April coming in for immigration and asylum. We are going to have it under Title VI covering police co-operation. We have this issue at the moment in the Council of this safe countries of origin list, which they have put off adopting because they cannot agree until they have QMV next April. I think in the longer term that the idea that just because you have 25 Member States there is a problem reaching decisions will disappear. When it comes down to a political level it is increasingly going to move to QMV, it is going to move therefore to co-decision with a bit more parliamentary input. In terms of organising working parties, it is a practical difficulty. I do know that the Council is having a problem with recruiting enough translators. There is literally a log jam of producing all the proposed legislation in all the 15 or 16 languages now. This is a short-term technical problem.

Q322 ***Earl of Listowel:*** Mr Bunyan, could you let us have your views on the role of the Counter-terrorism Co-ordinator, please?
Mr Bunyan: I think it is obvious from what I said earlier that I think there is a clear need for someone to carry out that role. Prior to 11 March a lot of areas just were not covered and one can say that the report I am talking about is extremely detailed and everyone could see there was a need for co-ordination within the Council. One hopes that happens. I think the danger is not to the post itself, the danger is—as one has hinted to some extent over the ad hoc groups and over the SitCen situation—that the Council starts to develop operational powers. I do not know how this Committee feels about this; this is a constitutional issue. In other areas, it is the Commission which monitors what happens at a national level. Such operational powers that exist are exercised by the Commission largely. When you are moving into the Second and Third Pillars you are seeing the Council

exercising operational powers. In other words, the Council is not just developing policy and advising politicians on what to do; it is actually in some areas co-sharing the operational aspects with the Commission and with the Member States. I do not think that most people are aware that this is what is happening. Obviously, logically, it is more obvious in the military field because you have SitCen and you have a European Defence Agency. There is a clearer structure in the Second Pillar because people have seen it, but they are not seeing the structure, as it were, developing within the Council itself. That, I think, is of some concern partly because of accountability and partly because I do not think that most parliamentarians are aware that that situation is developing.

Q323 ***Earl of Listowel:*** You mentioned the 7 March report. I am sorry I must have missed the full reference earlier. Where did that originate from?
Mr Bunyan: From the Council. It has not been published. It is not a report that we will publish either because one has to be sensitive to what happened on 11 March and therefore one can allude to some examples from it but it might not be responsible to actually produce that report, given what happened only three days later.

Q324 ***Chairman:*** Mr Bunyan, we feel certainly that you have an unparalleled ability to get documents before anyone else does! We envy you this great ability. Statewatch I feel should be commended for the work and the scrutiny that you do on all our behalves in the UK and I would personally like to thank you very much for that. We understand that you have been nominated for an award in the European Parliament.
Mr Bunyan: No, it is the "European Voice". Apparently I am one of the 50 most influential people in the European Union this year!

Q325 ***Chairman:*** We are not at all surprised. Could I thank you both very much indeed for coming and talking to us? Whenever you give us evidence it is always very concise, it is always very succinct and it is a great pleasure to have you come to give your views to this Committee. Thank you very much again; we have very much welcomed your evidence this morning.
Mr Bunyan: Thank you.

WEDNESDAY 1 DECEMBER 2004

Present
Avebury, L
Caithness, E
Dubs, L
Gibson of Market Rasen, B
Harris of Richmond, B
Listowel, E
Ullswater, V
Wright of Richmond, L (Chairman)

Memorandum by International Criminal Police Organization—INTERPOL

SECURITY FOR PROTECTING ONE'S COUNTRY MUST BEGIN BEFORE THE CRIMINAL ENTERS

To be safe, the UK, the European Union and all countries must strive to prevent local criminals from escaping internationally and international criminals from crossing inside any one country's borders. Interpol believes that the best way to achieve this goal is for police to share information about suspected criminals, wanted fugitives, and the tools of their trade. Interpol facilitates the exchange of this critical police information among its 181 Member Countries through a network of Interpol National Central Bureaus each of which is 100 percent controlled by the relevant Interpol member country. The UK, for example, has an Interpol National Central Bureau housed at NCIS and all UK police services can seek assistance with crime investigations that have an international element through the UK Interpol National Central Bureau located at NCIS.

Interpol also provides a sophisticated communications network which is required to permit the rapid exchange of information by police around the world, and since 2003 Interpol has been putting in place a state of the art secure global police communications system called I-24/7. Just this month (September, 2004), Sir John Stevens, Commissioner of the Metropolitan Police Department, was so impressed with the potential of Interpol and I-24/7 that he entered into a special agreement with Interpol to ensure that through I-24/7 the Bobby on the Beat in London could have direct access to Interpol's global databases on suspected terrorists, stolen passports, international fugitives, international criminals, etc. The Metropolitan Police Department now joins 116 Interpol National Central Bureaus worldwide and the New York City Police Department by permitting its police officers the ability to quickly consult Interpol's rich global databases. Interpol applauds the UK's plan to eventually connect all of its police departments, border control points and other law enforcement agencies to Interpol's I-24/7 network.

In addition to providing access to a network of 181 member countries to its global databases through a state of the art secure communications system, Interpol provides operational police support to its member countries on specific cases and crimes. Indeed, one of Interpol's principal tasks at its General Secretariat in Lyon, France and in its sub-regional bureaus in South America, Central America and Asia is to develop expert knowledge about international crime, and to provide expert operational advice and support to its member countries' police services. However, Interpol's advice and support must not simply help police services to respond quickly and effectively to crimes and emergencies as they occur which it does through its Command and Coordination Center and Incident Response Teams. It must also enable member countries to plan the disruption of terrorist and trans-national crime organizations: to get one step ahead of the criminals. Because of this, Interpol's knowledge must be both broad and deep.

Concrete examples are provided below as to how Interpol's secure Global Police Communications System (I-24/7); its global databases of suspected terrorists, stolen passports, international fugitives, international criminals, etc.; and its commitment to operational police support for its 181 member countries constitute **three core functions** that the UK must take advantage of and must support—if UK citizens are to remain safe from serious international crime.

1 December 2004

I. Core Function: Number 1:

I-24|7—Interpol's Secure Global Police Communications System Helps to Connect Police Worldwide

Interpol believes that by connecting police worldwide Interpol helps to secure the world. I-24/7 permits police access to Interpol databases from any point in the world, and it permits police the flexibility to communicate the existence of arrest warrants and to exchange photographs, fingerprints, names and other important information in a secure, fast and easy way. Since March 2003, Interpol has been connecting its Member Countries to I-24/7. In little more than a year and a half, 116 countries already have been connected, and over 3 million messages seeking important information for police have been exchanged for the first time in any calendar year—an 82 per cent increase over 2002.

II. Core Function: Number 2:

Interpol's Databases Help Member Countries Police Services to Identify Terrorists and Dangerous International Criminals

1. Assume that the UK wishes to determine whether the name or photograph of a suspected terrorist is known to police anywhere in the world, what database will permit the UK to determine the answer? Interpol's Global Database of names and photographs of suspected terrorists. **(With over 90 countries participating worldwide, Interpol has increased the number of names in its suspected terrorist database by over 1,500 over the last two years.)**

2. Assume that a terrorist or dangerous criminal possessing a stolen passport from inside or outside the European Union wishes to enter the UK, what database will alert the UK that the passport is stolen? Interpol's Global Database on Stolen Travel Documents. (**This database was created in 2002 with only 2 countries participating and a few thousand passport numbers. It now has 51 member countries participating and over 1.8 million stolen and lost passport numbers. The G-8 and the European Union have designated Interpol as the place to house the world's stolen and lost passport database.)**

3. Assume that a "Bobby on the Beat" stops a non-UK national for questioning, what database will alert the him or her that this person is in fact a suspected terrorist wanted for arrest internationally or simply whether the person is known to police? Interpol's Global Database for International Fugitives. (**Over the last two years Interpol's Member Countries and National Central Bureaus have increased the number of international fugitives arrested by 70 percent—reaching for the first time 2,000 plus arrests worldwide during 2003. With regard to the category of suspects known internationally, there were 2,697 positive hits in Interpol's databases of persons known to police in 104 different countries.)**

4. Assume that the UK arrests a person for a minor or serious crime and the UK wishes to know whether this person is whom he claims to be, what database will alert the UK that this person is in fact a wanted murderer or terrorist known under the same or different name? Interpol's Global Database of fingerprints. **(Interpol's fingerprint database of criminals investigated internationally contains 40,000 entries.)**

5. Assume that in connection with a highly sensitive investigation the UK wishes to determine whether any other suspected criminals used same phone number, address, etc., what database will give the UK this answer? Interpol's Global Database of phone numbers connected to criminal investigations. **(Interpol has in excess of 100,000 phone numbers and thousands of addresses queried by Interpol's Member Countries in connection with criminal investigations.)**

6. Assume that the UK recovers a DNA sample in connection with an investigation of a suspected rapist or child molester whose identity is unknown, what database would advise the UK whether that DNA sample is known to police somewhere in the world**?** Interpol's Database of Anonymous DNA profiles provided by participating countries' police forces. **(Interpol's DNA database contains no names. It is like an unlisted telephone number; no one at Interpol knows to whom the number belongs. It is Interpol's newest database. While its content is small in number, Interpol already has had its first match. A positive hit tells two countries that the same suspect could have committed crimes in two different countries. Interpol's maintaining this database without names will ensure the greatest data and privacy protection possible.)**

III. Core Function: Number 3:

Interpol's Operational Police Support Function Helps Member Countries to Prevent Serious Crimes and to Respond to Terrorist Incidents

7. Assume that a disguised weapon such as a pen gun, beeper gun or cell phone gun is recovered by security personnel at an airport or international institution, what organization would be able to issue a worldwide alert to police forces and international institutions within a short time of receipt of such information? Interpol through issuance of its Orange Notice Security Alerts. (**The Orange Notice Security Alert was created by Interpol in response to the series of parcel bombs sent to European Union institutions.**)

8. Assume that there is a major criminal incident or that terrorists strike somewhere in the world, what international police organization will offer to send a team to the site of the attack in order to provide support to the Member Country concerned and to ensure that wanted persons notices are issued; databases are checked; relevant warnings are issued and analytical reports are generated where appropriate? Interpol's Incident Response Teams. **(During the last two years, Interpol has sent 13 Incident Response Teams to 12 different countries. Interpol currently has teams in place in Bangledesh and Indonesia.)**

9. Assume that a Chief Constable needs help providing evidence in an illegal trafficking in human beings case, but he or she has no officer who speaks the particular dialect of Chinese needed, whom can the Chief Constable contact? NCIS, which would seek assistance from Interpol. (**In fact, the UK received help from an Interpol officer on just such a case.)**

10. Assume that there is a dispute between two countries about whether a certain finger mark lifted at a crime scene is the finger mark of a particular suspect to what international police organization could either country turn for an expert opinion? Interpol. **(Following the 11 March 2004 terrorist bombings in Madrid, the FBI and Spanish National Police disagreed about whether a particular finger mark was that of a lawyer in the US. Initially, the FBI identified the lawyer, but later admitted the mis-identification—blaming it on the quality of the electronic finger mark image transmitted by Spain. The FBI's explanation caused reverberations among police worldwide; so Interpol sent a two person team to Spain to review the evidence and determine whether the quality of the electronically transmitted image was sound. Interpol concluded the electronic image could not justify the misidentification.)**

IV. Conclusion:

The world of policing has changed since 11 September 2001 and 11 March 2004. Today, no responsible or prudent police investigator should consider a case closed until he or she has consulted Interpol's global databases. Without consulting Interpol, the police investigator would not know whether the suspect under investigation is known under any other name in another country; whether the suspect is under criminal investigation by another country's police service; or whether the suspect is wanted for arrest by another country for a more serious crime. Interpol has scores of examples proving this point. The most recent example concerns Denmark, which transmitted Interpol the fingerprints of a suspect arrested for a non-violent crime, but whom Interpol's fingerprint experts determined was also wanted for arrest for murder under a different name by a European country that is not part of the European Union.

This last example proves the futility of only cooperating within the European Union and of building up only national and European Union police institutions. Currently, the European Union appears to believe that it should concentrate **only** on national and European police institutions to keep Europe safe from terrorism, transnational crime and violent crime. In fact, national police and European police institutions share one common weakness. Neither can fight international crime successfully unless Interpol is used. Indeed, for citizens inside European Union borders to be safe, police and border control need to know whether the person who wishes to enter the European Union is suspected of having committed a crime anywhere in the world; is wanted for criminal prosecution by another country or is in possession of stolen travel documents from any country in the world. Only Interpol can provide this information systematically and rapidly in a cost efficient manner. Only Interpol can provide the UK and European Union Member Countries with the kind of operational police support that is needed to prevent or solve crimes whose origin is inside or outside the European Union.

Interpol and its three core functions provide the UK and the European Union with a unique set of services and added value that are priceless. At the highest levels of government, the UK and the European Union need to begin to take a more profound look at Interpol as part of the UK's and the European Union's strategy to keeping both the UK and the European Union safer from terrorism and other forms of serious transnational

1 December 2004

crime. Moreover, as resources get scarcer and as governments seek to avoid unnecessary duplication, the UK may find that investing in Interpol provides it with more financial leverage. For example, if the UK wants a UK police agency to produce a global database, its taxpayers would have to pay 100 per cent of the cost; if it asks a European Union Police Institution, its taxpayers would have to pay X per cent of the cost, but if it asks Interpol the cost could be spread over 181 member countries and the percentage would only be Y percent. In short, Interpol is the essential link to an effective UK and European anti-crime strategy.

20 September 2004

Examination of Witness

Witness: Mr Ron Noble, Secretary General, Interpol, examined.

Q326 ***Chairman:*** Mr Noble, welcome. It is very good of you to come from Lyon to give evidence to this Committee. I would also like to thank you very much for the written evidence which you sent to us some time ago. As I think you know, this session is being televised; it is on the record. For the benefit of any members of the public or those who are watching I should record the subject of the inquiry. It is an examination of a number of proposals designed to strengthen EU counter-terrorism activities, particularly through much more extensive data exchange. These proposals raise important issues relating to, among other things, data protection and the institutional arrangements within the EU for combating terrorism, which is of course a global problem not confined to the EU. This session gives us the opportunity with your help to look at it in a much wider perspective. We have all recorded any interests that are relevant to the inquiry and they are available at the back of the room. I am not proposing to ask members of the Committee to repeat their interests in this session. Would you like to make an opening statement before we come to the questions?
Mr Noble: Yes, my Lord Chairman.

Q327 ***Chairman:*** Please do.
Mr Noble: My Lord Chairman, my Lords, it is an honour for me to have been asked to provide evidence to this distinguished committee. To be safe the UK, the European Union and all countries must strive to prevent local criminals from escaping internationally and international criminals from crossing inside any one country's borders. I say this because the world of policing has changed since 11 September 2001 and 11 March 2004. It is the view of Interpol that no responsible or prudent police investigator should consider a case closed until he or she has consulted Interpol's local databases. Without consulting Interpol a police investigator would not know whether the suspect under investigation was known under any other name in another country, would not know whether the suspect was under criminal investigation by another country's police service or whether the suspect was wanted for arrest by another country for a more serious crime. Interpol has scores of examples proving this point, but the most recent example comes from the UK. The UK sent to Interpol sex crime scene DNA samples of unknown suspects, so no privacy issues were at stake here. The UK's initiative was rewarded by their receiving 12 positive hits based on unknown DNA samples stored at Interpol. Now the UK and other Interpol member countries know that the alleged suspects may be committing sex crimes not only in the UK but in other countries as well. This last example proves the necessity of the European Union member countries' police forces co-operating not only nationally and regionally but also globally through Interpol.
Currently the European Union appears to believe that it should concentrate only or principally on national and European police institutions to keep Europe safe from terrorism. In Interpol's view this would be a mistake. In fact, national and European police institutions share one common weakness: neither can fight international crime successfully unless Interpol is used. I will use the UK again as an example. In the last year the UK has made over 10,000 name inquiries using Interpol's databases and it has received almost 5,000 positive hits from 149 different countries, clearly demonstrating the need for European member countries to look both inside and outside Europe for help. I will close by saying that Interpol has 182 member countries. It has received strong support from the UK, NCIS in particular, and from the UK's own Interpol National Central Bureau (NCB). Our most significant partners are from the European Union but sometimes when the European Union looks for help it looks only at European institutions and national institutions and my hope today is that after my giving this evidence you will consider Interpol an additional tool to use in keeping this country safe from terrorists and other dangerous criminals.

Q328 ***Chairman:*** Mr Noble, thank you very much. That is extremely helpful. Could we talk a bit about the basis of Interpol? Do you have a constitution? Are you accountable and, if so, to whom? How do

your members work together in practice? You have given us some examples, very helpfully.
Mr Noble: Interpol is a 182-country organisation. We have a constitution that has a number of articles, the most important of which is that we are forbidden from being involved in matters of a political, racial, religious or military nature. We have a one country, one vote system. We have no security council and no country has a right of veto. We are overseen by a 13-member Executive Committee and that includes the Head of the Interpol NCB in the UK, Mr Ken Pandolfi. Each Interpol member country has an Interpol National Central Bureau that is 100 per cent controlled by the member country concerned. Any rule or any resolution or any decision that we take must be consistent with the individual sovereign member country that wishes to execute it.
We have three core functions. One is that we provide the world's police forces with a secure global communication system that allows them to share messages with any country they choose, so if the UK wishes to send a message to only three Interpol member countries then only those three Interpol member countries will receive the message. The sender of the information controls which countries have the right to access the information in question. That is, the sending country decides what other countries can receive it and can make access to the information even narrower by having a particular working group established with identifiable persons given authorization to access. For example, the UK is a strong participant in Interpol's efforts to fight the sexual exploitation of children over the internet. The working group involved in that includes identified individuals who have their own secure network that others cannot have access to because of the secure nature of the information concerned. Finally, we have our General Assembly that is the ultimate arbiter of any decision taken by the organisation. We try to function by recognising that it is important to allow those countries which wish to co-operate to co-operate. Those countries whichdo not wish to co-operate are not required to do so on whatever cases or situations they choose not to.

Q329 ***Chairman:*** How much of Interpol's activities at present are related to terrorism and counter-terrorism as opposed to other forms of crime? Could I ask a supplementary on that because you said that your constitution excludes religion? Is this in practice a constraint in meeting the threat of Islamic terrorism?
Mr Noble: What our constitution prevents is for us to assist the prosecution of someone for having violated a religious law. If a country were to say, "You cannot be a Catholic in this country", that is the kind of case we would not be permitted to work on. In terms of terrorism and the problems that our constitution poses in fighting terrorism, what we try to do is facilitate countries finding information out that helps them determine whether or not a person suspected of being a terrorist is in fact a terrorist or is not a terrorist We believe that, to the extent that our constitution prevents us from getting involved in political matters, that is a case-by-case determination that is very difficult, very time-consuming, and we try to make the best decisions that we can.

Q330 ***Chairman:*** If I could return to my question, what sort of proportion of your work at present is related to terrorism?
Mr Noble: It is difficult for me to put a percentage on it but I can give you examples by focusing on priorities. Our number one priority is fighting terrorists, terrorism and serious international crime. From Interpol's perspective, when Interpol receives a message requesting help in identifying a name or a phone number or an address, Interpol might not know whether the case is a terrorist case or an organised crime case, so what we try to do is help the member country determine what assistance it needs on a case-by-case basis because if the UK is looking for a murderer, a sex offender, a fugitive who has escaped, we have a Command and Co-ordination Center that we established to fight terrorism. We have incident response teams that we send to countries where terrorist attacks occur. We have sent 17 of those teams. We will circulate worldwide within one day a country's request to seek the apprehension of a terrorist. We have a Terrorism Task Force that we established, which between 2002 and 2004 added an additional 2,000 suspected terrorists to the list. Everything we do is tied to terrorism in some way because we are trying to help countries prevent terrorist acts. In terms of the budget I could not give you a percentage; I am sorry.

Q331 ***Chairman:*** Do you see yourselves primarily as a channel of communication between countries? To what extent are you doing analysis and political work?
Mr Noble: We have, as I mentioned, three core functions. One is to facilitate a member country's ability to communicate around the world when it is seeking information about someone, so yes, we do perform that function, but in the analytical area we perform a great deal of functions. For example, assume there is, as we had just last week, a case involving a suspected paedophile. We had a videotape of the person which also had a voice component to it. We extracted the voice and we used our global communication system to send the voice around the world to see if someone could recognise the accent to help us identify where this person was located. We sent an Incident Response Team to Bangladesh following a terrorist attack there and we

learned that they did not have a great case investigative structure for terrorist investigations, so we provided some help there. The final example I will give you is that in our Fusion Task Force we have working group meetings and, based on the information received in those working group meetings, analytical reports are generated. We provide three core functions but we also provide analytical support as needed and try to do it on the most important cases or the cases that seem to have the widest impact.

Q332 ***Baroness Gibson of Market Rasen:*** You said that it is up to the country that provides the information to decide to whom this information goes. Would there be any case where Interpol receives information, sees where the country wants to send it, and thinks, "Ah, there are other countries who ought to have this", and you would advise the first country accordingly? Would that ever happen?
Mr Noble: That happens frequently. I recall Christmas Eve 2002 when we received a notification from a member country that they believed there might have been a parcel bomb placed on a plane headed towards country A. They wanted the information only to go to country A but we believed the information was so important that it needed to go to a number of countries, so we contacted the sender of the information and we said, "We believe this should be shared more broadly", and they agreed and so we shared it more broadly. We also have countries that we know do not have strong bilateral relations, so country A might send us a message asking about person Z. Country B might send us information about person Z, but they say, "Do not send the information to the other country". We contact each country and we say, "You are interested in the same person. You must find a way to communicate with one another".

Q333 ***Lord Dubs:*** You have partly answered my question but let me just get the remainder of it on record. In your opening statement you gave an example of where there had been a sex offender and where you established, to help the British police, that there was evidence that that same person had committed offences in a number of countries. That slightly tells me how it helps the British police but it does not really get them very much further Is it a constraint on your operations if you cannot get more information in order to give more helpful information to the police force that has requested the information?
Mr Noble: If I could answer the first part, I would submit that it is very helpful. What was sent to Interpol were crime scene samples of someone unknown to the UK. By sending the crime scene sample to Interpol and by Interpol identifying other crime scene samples in other countries, those countries can get together and find out whether there are commonalities to it in order to help identify the person. With regard to sharing information, nationally, regionally and globally countries' police forces and intelligence services could be sharing more information; that is a fact. What we try to do is use example after example of where sharing information helps facilitate the protection of the country concerned in order to encourage that sharing of information to occur. There are, I would say, three barriers. One is lack of knowledge about what Interpol can do and how it does it. Another is a lack of willingness on the part of a member country to share information and the third is the inability technically or legally to share the information with Interpol. The example I would give you is in the area of DNA. Our database is of anonymous DNA samples, so there are no privacy issues, but we know one day in the future Interpol's database should include DNA profiles with some identifying information, like we have for fingerprints. I hope that has given you some comfort in terms of how it helped the UK but also recognising that there are barriers that do exist.

Q334 ***Lord Avebury:*** You have just said that police forces with intelligence services could be of benefit if both of them shared more information than they do on a national basis. Are there any rights of access to the Interpol database by services other than the police in any of the member countries, such as customs and immigration and intelligence services?
Mr Noble: The UK is one of the leading countries for extending access to Interpol databases beyond the Interpol NCB office. The UK's goal is in processing and implementing and extending it to all law enforcement services in the UK, including immigration, including customs, and also giving access to the intelligence and security services to the extent that they are engaged in criminal-like investigations. That is something that is currently under way in the UK and throughout Interpol member countries around the world.

Q335 ***Lord Avebury:*** You have mentioned some obstacles that exist to the provision of identifiable DNA material from investigations. Could you say what other obstacles exist to the effective exchange of information in respect of terrorism between agencies within countries and between countries?
Mr Noble: Between agencies within countries, my Lord, there is a problem of classification and deciding what information to classify and who has access to that classified information. Depending upon the rules and regulations and policies within a country there could be limits on the kind of information that is shared. Beyond the country, if we go regionally, the

intelligence services and many police services tend to be very concerned about information that is very sensitive getting in the wrong hands, and the nature of their training has been to prevent that from occurring; so they tend to share information with people with whom they have a good relationship or who come from countries with whom they have a good relationship. It is just the nature of it. The best way to overcome this obstacle is to say to someone in the intelligence service, "You have ten passport numbers that are associated with ten individuals that you believe are very dangerous and are suspected terrorists. Unless you input those ten stolen passport numbers in Interpol's database you will not know whether those ten are part of the five million that have been stolen". There is a fear to test the system and to search the system to determine whether or not someone who is of interest to you is known to someone else. The final obstacle is that there are a number of countries that have prohibitions on their police services or intelligence services working in other countries as a matter of law, and that has to be respected. From my point of view the greatest barrier is a lack of knowledge about what is possible and a lack of willingness to try. Those are what I consider the greatest barriers to international police co-operation and national police co-operation.

Q336 ***Lord Avebury:*** Is it not legitimate to have some fear that information will get into the wrong hands? Supposing that during the period when the Taliban was in control of Afghanistan they had been members of Interpol. Would people not have had reason to fear that if they had had access to the full range of Interpol information it would have got into the wrong hands?
Mr Noble: I think that is a fair comment but our response is that that shows that the entity involved does not know how Interpol works. The member country that controls the information can say, "It cannot be shared outside this group of countries", or the member country can say, "Send it only to person A or person B". There are levels of information, levels of classification. What we are saying is that a rule that you cannot share anything at any time is a wrong rule. The rule should be, "Let us look at the information, let us look at the risk and let us decide with whom we can share". The hypothetical example I would give you would be: assume that a country knows there is someone in possession of a bio-agent which, if it were released, could kill tens of thousands of people. We would want that country's police force or security agency to share the information with someone, not just keep it to itself. I am not saying the country should share it with everyone, but my starting point is, "Look at the information, look at the risk, decide what tools are available and then try to take the best decision that you can". However, I accept your point that not all information should be shared with all countries all of the time.

Q337 ***Lord Avebury:*** As you know, within the European Union there are proposals for enhancing access to information by law enforcement authorities and providing for what is called equivalent access, and also proposals to enhance the interoperability of the EU databases. Do you support those ideas and are they practicable and have they implications for Interpol?
Mr Noble: I strongly support the ideas. I believe that the interoperability issue it is going to be a very difficult issue to resolve and I believe Interpol has a role to play, especially on an interim basis. I will give you an example. Last night I came into the UK. I am unfortunately not a UK citizen and I was required to complete this immigration card. I was surprised that the immigration card did not ask me for my passport number. I know Interpol has a database with over five million stolen passport numbers. I say to myself, "If the interoperability does not work, if Interpol knows that there are over five million stolen passports that we have access to, if it has been proven in every serious terrorist incident that a fraudulent passport has been used, why would the UK not want to know my passport number?" Until such time as there is interoperability we are willing to let the UK download all of our stolen passport numbers.
What we are saying is that there is an interim step that can be taken. The UK is already taking it as it links to people who are wanted. If someone is wanted that person would not come into the UK, but assume there is an unknown terrorist in possession of a stolen passport. We need to find an interim solution to make sure that those people do not get into the UK. The example that I can give that is most compelling is that the former Prime Minister of Serbia, Mr Djindjic, was assassinated on March 12 2003. The person arrested for his assassination had a stolen Croatian passport that was blank until it was made fraudulent. That passport was used to get in and out of six countries in Europe, and Singapore, and was stamped 26 times by immigration officers. If that had been another head of state or if that had resulted in tens of thousands of people being killed, our citizens would never forgive us for not trying to give access to information that has no privacy issue because it is a passport number, in order to prevent someone from getting into a country or moving from country to country. I strongly support Europe's effort to share information and the UK's effort to share information. I say this sincerely on the record, and I have said it in speeches, that when it comes to sharing information nationally the UK is one of the leaders in the world. The UK is at the forefront of pushing me as Secretary General and Interpol as an

organisation to try to give countries more opportunities to share information.

Q338 ***Viscount Ullswater:*** In your very helpful written evidence you have described the various databases that Interpol operates. In fact, you listed by example at least six of them, and there may be more than that. What rules are in place governing the storage and deletion of data? Am I right in thinking that these databases are held centrally by Interpol or are they held in the 182 member countries, and how does Interpol validate the accuracy of the data that it holds?
Mr Noble: You are correct that Interpol does have centrally located databases. We satisfy the European standards, the global standards, for data protection. We have a commission for the control of Interpol files that consists of three representatives from data protection agencies throughout the world plus an Executive Committee member from Interpol. They do spot-checks, they make sure that the regulations that we have in place, which do satisfy international and European standards, are satisfied. We were certified by the International Data Protection Certification Agency. In terms of the accuracy of the information, that is the most difficult issue to resolve because what Interpol says is, "We will do our best to report accurately what a member country has told us". If a member country says that person A is wanted for murder we will communicate accurately what person A's description is, based on what we have received, and what he is wanted for. In terms of the proof to determine whether or not the person did commit murder, that is information we cannot verify, so what Interpol does is help member countries learn what other countries believe or have said about people of interest to them.

Q339 ***Viscount Ullswater:*** That is a very interesting answer because what I would like to pursue a little bit further is that obviously some of the databases contain factual information, including criminal convictions. You were talking about a suspect at one moment but, putting aside the facts of the case, obviously you do record criminal convictions against people and stolen passports. These are the factual side, but others are concerned with much more sensitive information, such as details of terrorist suspects. Are there special arrangements for handling the ones which are suspects and the factual ones?
Mr Noble: Yes, it is a very complex question. What I would say is that we say to member countries, "When you give us information, decide what other countries you would like to have access to that information and what other people you would like to have access to that information and only give us that information. If there is information that you are worried about being so sensitive that it might get to someone beyond that, hold that information back". If someone makes an inquiry of Interpol, we will say, "Contact the UK" or "contact Germany" or "contact Japan for further information". From our perspective, we try to put member countries in contact with one another about people who are of interest to them for having been engaged, or being suspected of having been engaged, in serious crime. It is not my goal to have the most sensitive information. My goal is to have identifying criteria that will help a member country decide whether the person of interest to it is the same person about whom another country has given us information. It is a very complex question. I hope I have at least aided you somewhat in understanding how it works.

Q340 ***Viscount Ullswater:*** I am sure it must be very difficult in practice to be able to organise that sort of structure.
Mr Noble: It is very difficult. That is why we have working groups where member countries share the ways in which they approach it. I will give you an example. You might not believe it initially but trust me that it is true. One of my biggest concerns as Secretary General was to have information about a suspected terrorist that I was not permitted to share with another country because I knew that, if that information had been shared and it could have prevented the killing of scores or thousands of people, no one would forgive me or my organization, for the reason that you mentioned, that we have to ask, "Can I share it?" We said we would ask our member countries to share information on suspected terrorists that we could share with all countries. At the first meeting we had, 39 countries attended—all suspicious, all believing that this would not work, all very critical of the idea, calling it not realistic. Now, two years later, we have 117 countries participating and over 2,000 names of suspected terrorists we did not have on our database before. Depending upon who the person is, we might have a photograph, we might have fingerprints, we might have specific details, it depends, but at least we have names that we did not have before. Now at these same working groups there are efforts and opportunities for us to exchange more information. With our Fusion Task Force which concentrates on fighting terrorism, every country knows that if they give us a name, we share it with everyone. If you do not want to share it with everyone, in the margins of the meeting you can exchange information; you can give out contacts for later. If it is in Interpol's database as a result of our Fusion Task Force, we share it with everyone. So far, it has proved quite successful.

Q341 ***Chairman:*** May I revert to a question which I think was asked but I am not sure I heard an answer?

Do you have standing rules about the deletion of information?
Mr Noble: Yes, we do.

Q342 ***Chairman:*** I apologise if you have already answered that.
Mr Noble: No, my Lord Chairman, you are correct, I did not answer it. I apologise for not having done so. We have specific rules concerning the processing of police information: specific deletion of rules, specific updating of rules, et cetera. The Commission for the Control of Interpol's Files, an independent entity, oversees the way in which we function and each year is required to give a report to our membership about whether we have been in compliance with the rules or not.

Q343 ***Lord Dubs:*** Mr Noble, may I go back to the question of stolen passports, to which you referred earlier? I fully understand the significance of the point you made about stolen passports and the need to have such information. This is my question. The EU has currently under consideration proposals requiring Member States to transfer data on lost and stolen passports. Is this necessary or do you not already have enough information from Member States provided to you on an individual Member State basis? In other words, do you need an EU system to improve on the present position?
Mr Noble: We believe that the EU, which has in its Schengen Information System approximately 10 million stolen passport numbers, should share that information with Interpol. The EU has taken a decision to that effect. We embrace that decision and we believe it needs to be implemented as soon as possible. We currently have 5,589,568 stolen passports and the largest contributing countries are from the EU. We say that it is important to the EU to know whether the stolen passport is being used in the EU or outside the EU. That is why an EU system alone will never work; it must be a system that is global, where the EU has access but other countries have access as well. That is what we have built and that is what we have given countries access to around the world.

Q344 ***Lord Dubs:*** To be sure that I have understood that, are you saying that what you want is close co-operation between Interpol and the Schengen Information System or are you saying that the Schengen Information System on its own does not do anything that Interpol cannot do anyway, provided the individual Member States give you the data?
Mr Noble: The Schengen Information System is a good system. It works well and it allows the European Union to do things that it otherwise could not do. There are some items in the Schengen Information System that do not need to be in the Schengen Information System, or do not need to be only in the Schengen Information System: stolen passport numbers is an example. We believe that, if you use our stolen motor vehicle database as an example, the EU Member countries and countries around the world would put the stolen motor vehicle information in once; that same entry would go to the Schengen system and to the Interpol system. A bobby on the beat stops someone; she puts in the identification number; it comes back a hit whether it is from the Schengen system or from the Interpol system. I am submitting that where the stolen travel document database is concerned, the Schengen Information System does not need to have that database. If it has it, it can, but it does not need to have it. We can provide the same information coming from Interpol. I do not want to get into the fight with the Schengen Information System and say, "I want to take something from you". I am simply saying that when the information is entered, it should at least go to Interpol. If it goes to Interpol and Schengen, that is all right but it should not only go to Schengen. I hope that has been clear—and has kept me out of trouble!

Q345 ***Chairman:*** Have you noticed, since the enlargement of the EU to 25 Members, any significant difference in your relationship with the Schengen Information System?
Mr Noble: No. There is something about joining a new club that makes it seem more interesting than being a member of an existing club. It is not true here in the House of Lords, I know! Every day I am fighting in Interpol to get member countries to send me their best police officers to help keep their countries and their regions safe. I have 70 countries represented in Interpol offices around the world. When the EU says to countries, "Join the EU. You need to pay dues. Send a liaison officer", they all do it. They have a one hundred per cent success rate. When I advertise the number one position for specialised crimes at Interpol, and because we are not a wealthy organisation, I say, "Member country, you have to pay for it", I might get three applications, maybe five applications. That is for the head of a specialised crime unit for Interpol. I know that if I could pay like Europol pays, I would get 70 applications or 700 applications. I have noticed that there is a movement of personnel towards the EU and, since there are scarce resources, the movement tends to come from Interpol so that we do not have the depth in personnel that we once had; we do not have the political support that we once had. Yet, when the March 11th terrorist attacks occurred in Madrid, Interpol was on the ground with the Spanish authorities helping them process information, sending a finger mark around the world, producing wanted persons' notices to keep Spain and Europe

safer from the other attacks that were planned. When the countries got together afterwards from the European Union, the reaction was to find a European Union solution instead of saying, "What other institutions do we need to reinforce and build up?" Being invited to testify before you today for me has been an honour because my member countries will say, "There is a legislative interest in the work of Interpol". Before coming here, I met with the Interpol staff at NCIS to speak to them and I proudly said, "Your House of Lords invited me, your Secretary General, to give evidence and that has never happened before". There is no problem in terms of the Schengen Information System as a result of the expansion of the European Union. There is just a problem in scarce resources being even scarcer as it relates to Interpol.

Q346 ***Lord Avebury:*** Would it not be a good idea then if more of the top posts at Interpol were paid for out of the subscriptions of Member States instead of, as you say, having to be funded by an individual member that supplies that officer?
Mr Noble: I wish I had written that question for you because my statement is: yes, it would be but at Interpol prior to September 11 we were not as vibrant, as operational. The threat was not understood by the world as it has been understood since. Our budget has grown, thanks to a person whom I am going to have to identify here, John Abbott. He was then the Director of NCIS who supported the most significant budget increase we have had in our history. In percentage terms, it is high; in pound terms, it is really insignificant. If I had a dream that could be fulfilled and I could have paid posts and still remain in office, then I would say, "Yes, that is the model we should move to". That is the model NCIS has moved to. That is the model anyone would move to if you wanted to be able to hire the best people. I say this with all due respect to my member countries.
Imagine you have a person in your country who is a problem for you but you have only so many offices you can send the person to and he or she has been through all the offices. You say, "I have just received a letter from the Secretary General of Interpol saying he needs more people". They might say, "Ron, I have just the person for you". That does not happen but if you have a need for bodies and you cannot pay the institution involved, then you are not going to be able to be as selective as you otherwise would. That is why we get three applications for jobs and Europol gets 70 applications for them. If I could pay, we would get 700 applications.

Q347 ***Viscount Ullswater:*** Before we leave this Schengen Information System area of questioning, I would very much like to ask: are there any databases in the Schengen Information System that are not shared with Interpol? I am thinking of Eurodac perhaps?
Mr Noble: Everything in the Schengen Information System is not shared with Interpol. We are not authorised to have access to anything in the Schengen Information System. If we have the information, it is because a country from the European Union has sent the same information to Interpol. From Interpol's perspective, what I have done as Secretary General is to say to Europol, "You have access to all of our databases". I have a Europol Liaison officer in Interpol headquarters in Lyon. We have told the European Liaison officers who work in Europol that they can have access to all of our databases. We have joint working groups. I have given access to all our information to the Schengen Information System. We are not an authorised entity for any information in the Schengen Information System. That is why the Schengen Information System has about 10 million stolen travel documents and we have five million for the whole world, which means that when a country asks us whether a particular passport is stolen, if the country is outside of Schengen, it cannot ask Schengen. If it asks Interpol, we say no, but we are then giving back many false negatives. We believe that there must be some information in the Schengen Information System that Interpol should have access to, the first of which would be stolen travel documents. Also, with regard to euro counterfeiting, we know that the euro counterfeiting threat will be a threat based on evidence outside the European Union and not just inside the European Union. I think there is a great opportunity there for the sharing to occur both ways, my Lord.

Q348 ***Baroness Gibson of Market Rasen:*** You mentioned earlier about sensitive information falling into wrong hands. Can you tell us about the data protection arrangements that Interpol has?
Mr Noble: We have data protection rules which make it clear that the country sending the information dictates to what countries it can be shared and the limitations on where it can be shared after that point. A member country could say, "This information can only go to the NCB of country A, or country B, or country C". Then it is up to the NCB in the country concerned to make sure that that request is met. As it relates to information that is sent to the general secretariat in Lyon and we are told "don't share this with anyone", we do not share it with anyone unless it is authorised. Our Commission for the Control of Interpol Files examines us and does spot checks to make sure we are adhering to the rules and regulations on information that we receive. It is a very rigorous process and it is something that we have to be very conscious of because the one time that

we breach that, it will undermine the willingness of all countries to share that information with us. So far, over the last four years, each assessment and review we have received under the Commission for the Control of Interpol Files has been a very positive review. That is not to say that there are not areas identified where we need to improve, but, in terms of respecting our rules and regulations, we have been satisfying very high standards.

Q349 ***Baroness Gibson of Market Rasen:*** That is very helpful. Can you speak about the recent comments of the UK Information Commissioner that the limited data controls on the data transmitted to Interpol affect Interpol's effectiveness?
Mr Noble: I have learned a lot from attending international meetings with UK citizens. There is an expression that at the beginning I thought was a compliment but by the end I learnt was not. The person would say, "That sounds very interesting". I believe people who make statements like that are sincere in their belief but they are not familiar with Interpol's rules and regulations and how we have changed over the last four years. I really believe it is too easy to say that there are legal barriers to sharing information because we know it is a problem that exists nationally and regionally. I believe Interpol has demonstrated over the last four years that more people have been arrested than before, that information is being shared about more people than before, that we have more countries co-operating than before. I believe we have made great progress but a smart person can always find something about Interpol that does not sit well with a specific issue. Am I prepared to respond to your question? The short answer is: I do not agree with the statement made by the distinguished Information Commissioner.

Q350 ***Earl of Caithness:*** Mr Noble, in your written evidence to us you said that was futile for Europe just to co-operate within itself. How would you like to see the co-operation between Interpol and the EU expanded into a better basis?
Mr Noble: Any time the EU considers a crime problem of importance to the EU, I would like Interpol be invited to the table, whether as an observer or as a participant, in order to share our ideas and views with the EU entity involved. That has happened with the European Police Chiefs' Task Force. We have recently been included as an observer and we have been able to make contributions. I believe that the EU needs to think about Interpol being one of many tools available to it which the EU needs to make use of, to support, and to criticise where appropriate. I believe that is just not happening at the highest levels of Member countries. This is not a criticism; it is a natural reaction that countries have to problems. You talk to your national police officers or you talk to institutions that you control. Since Interpol is not controlled by any political entity, we do not have the support but we also do not receive criticism, but if you do not have the support and you do not receive criticism, you are not going to improve. I would like recognition by the EU along the lines of health. If there was an international health problem, WHO would be considered. Or, if there was an international monetary problem, it would be the IMF or the World Bank. If there is an international crime problem, it should be Interpol. I do not want to control anything. I simply want us to be considered an available tool that needs to be managed in the correct way in order to provide the best services possible.

Q351 ***Earl of Caithness:*** Taking that a little further, if you are looking at the work of Europol and at your work, do you see your work as complementary or are you working on the same footprint and therefore you are duplicating?
Mr Noble: That is a very good question. If Europol did not have the name Europol, if it was called the European Police Agency, then I would say that we would serve Europol like we would any other client we have, whether it is the FBI, NCIS or the National Crime Squad. Europol is not at all related to Interpol; it does not follow the same rules and regulations, and it does not have the same mission statement. It should not be thought of as a sub-set of Interpol, because it is not. When I think of Europol, I say, "Europe wishes to share information. It has created this structure, this entity, and this entity needs our support like national police institutions do, and so we give Europol access to databases, as we do our Interpol offices". We have projects that we work on together, as we do with our member countries.
But Europol is not a 24 hours a day, seven days a week operational police support organisation like Interpol. It has a different mandate and it is still looking for its mission statement; it is still looking for its identity. Our identity is very clear. Europol is an entity that we work with and we want to support, but it is far different from Interpol.

Q352 ***Lord Avebury:*** I was wondering whether you have regular meetings with the Counter-Terrorism Co-ordinator and whether that is a way of preventing this duplication or overlap?
Mr Noble: You are speaking about whom specifically?

Q353 ***Lord Avebury:*** The European Counter-Terrorism Co-ordinator, Mr de Vries.
Mr Noble: I have not had regular meetings with him. I have had one very fruitful meeting with him to try to make sure that he recognises that we have an

important role to play, but the European Union, when it tries to resolve a problem, tends to look at its own intuitions. It does help to have meetings. We try to have meetings. The problem I think is much more structural than based on personality, to be honest.
Chairman: You and other members of the Committee might like to have a look at yesterday's *Financial Times* in which there was an article by Mr de Vries about his job.

Q354 ***Earl of Caithness:*** Would you like to see yourself more as a clearing house for information on crime so that you provide the database and then you let regional or local crime squads, the police, take the information? You seem to be saying that you make your information available to the Schengen Information System, to Europol. If they would do the same, they could get on and do their work better and you would have a bigger database as a result?
Mr Noble: I believe one of our core functions is to have the ability to provide database services to member countries around the world. That is definitely something that we are moving towards, and we are saying that to the extent that you want information to be shared accurately, quickly and efficiently, we should do that, but there are other functions that we perform in the area of providing operational police support. One example is that when there is a terrorist incident anywhere in the world, we send a team there to try to help them, not investigate the case nationally necessarily but to make sure the links internationally go the way that they should. We have the ability to work in four languages 24 hours a day: English, French, Arabic and Spanish. We also try to develop standards for DNA, for fingerprints, for transmission, for the ways in which arrest notices are transmitted around the world. We have working group meetings on anti-terrorism and human trafficking. A success story for the UK is a case in the US where a company was selling the right to have access to images of children being sexually exploited for $29.95 a month and there were subscribers from around the world. Interpol got the data, 60,000 names, divided it into country files and sent it to our member countries. From that, the UK executed over 500 search and arrest warrants. It was called in the UK Operation Ore, but you did not hear that Operation Ore began with Interpol Operation Landslide. Had the US not sent the information to Interpol, had Interpol not analysed it and sent it to member countries, Operation Ore might not have happened. Yes, databases and data services, operational police support and putting in place a global communication system, are functions in which I believe Interpol has an important role to play for the EU, for the UK and for the world.

Earl of Caithness: That is very helpful. May I broaden this a little bit for you to give the Committee a brief comment on how you see the rest of the world? We have talked a lot about the EU but how is your own country of America responding to Interpol and the other countries?

Q355 ***Chairman:*** Could I add a supplementary to that? Could you tell us, if you know, of cases where information provided by Interpol has actually ended up in the wrong hands? Please answer Lord Caithness's question first.
Mr Noble: I have battles with the US to get the US to co-operate with Interpol like you would not believe. It is just a day-to-day fight. I used to be in charge of four of the US's largest law enforcement agencies. I have strong personal relationships with people in those agencies. It is a fight. I have said this publicly: the US believes that it can have bilateral relations and multilateral relations that can solve just about any problem. Here is how bad it was. It is not this bad now. Following September 11, in order to find out who the US was searching for arrest worldwide, we would monitor all public sources—television, internet and newspapers—to see what names were listed. Then we would contact the US and say, "Please ask us to look at our databases to see whether or not these names exist". It took the Attorney General of the United States (the Honorable John Ashcroft) coming to Interpol headquarters and my saying to him, "There can be no security risk if you had a press conference". He agreed. He did not know about the problem it. The next day, the FBI and other institutions got the message. Just recently, with the Van Gogh murder in the Netherlands, we contacted the Netherlands and asked, "Do you have any names? Is there anything you would like us to check on our database?" The answer was, "No, it is too sensitive". We read the newspaper the next day or two days later and we saw the names in the newspaper. We ran those names against our databases and then said, "We have information on some of these names. Please share more names with us". It is just a day to day struggle to get countries to do internationally what they do naturally nationally. Nationally, when you arrest someone, you check his or her name for fingerprints against national databases. It just happens by rote. Taking it the next step does not usually happen. Denmark is one of our strongest co-operating countries. Every time Denmark arrests someone, even if it has all the evidence they need, it sends the fingerprints, the name and a photograph to Interpol. Just as I was preparing my testimony, Denmark sent us information about a drug trafficker about whom Interpol had information that he was wanted by Serbia for arrest on murder.

From Interpol's perspective, what people do not realise is that you never get a negative answer from us. If you send us the name of someone and we say he or she is unknown to Interpol, that response would be valid only as of that date, but your inquiry goes into our database, the trace of it. If, within five years, we receive another request about that same person, we can say, as we did for Serbia, "The person you asked us about two years ago has just been arrested by Denmark. Please contact them directly".

Africa: we believe that in order to communicate, you have to have a communications system in place. Because we are not a wealthy organisation, we designed this global communications system that relies on secure internet encryption we can put in our member countries. We got a number of countries to pay for large aspects of the system themselves in order for us to be able to pay for Africa because their telecommunications system is not what it should be. In Africa, we are going to put in place a satellite communications system for Africa. We connected the first country, Tanzania, to this last week, which means that if there is a problem in an African country or an African country has a view, they have a communications system with us.

I came back from Pakistan recently. We know Pakistan is on the front line of the anti-terrorist efforts. Pakistan has one of the most robust border control systems in the world. Pakistan can now obtain the name, photograph and passport number of anyone who enters and leaves the country. Over the last year, Pakistan has given member countries around the world 790 positive hits of people who have entered or left Pakistan who were interesting, but Pakistan wants to extend this beyond the NCB to their provinces and to the drug traffickers. They do not have the money. They have asked Interpol for the money. I tell them that we can take a system from one of our offices here and we will find five or six systems to give to Pakistan. I say the world should give Pakistan the money to put these systems in place because if the terrorists can be caught in Pakistan, that will keep the rest of the world safer. The world that we live in has 182 member countries, some wealthy, some not so wealthy, some who co-operate, some who do not co-operate. We try to keep lifting the playing field, thinking that that one case can make the difference and then promoting that activity. That is why this opportunity helps.

With regard to your question, My Lord Chairman, I am not aware of any information that has come to Interpol getting into the wrong hands. I am also not aware of information in the country from where I come getting into the wrong hands, but it is that fear of getting into the wrong hands that the intelligence community and the law enforcement community use time and time again for not sharing information.

Q356 ***Lord Dubs:*** You mentioned that Denmark was a particularly good country in terms of being diligent in supplying you with information. Would you be prepared to hazard a comment about how good Britain is, taking Denmark as the yardstick? I do not want to get you into trouble.

Mr Noble: I would like to answer your question slightly differently from the way in which it was posed. In terms of our database of names of wanted persons or suspected criminals, the number one country in the world in terms of searching that database is the UK. The country that has received the most positive hits has been the UK. This is not going to be a positive statement but it is a fact: in terms of the country that has the most stolen motor vehicles on our database, that happens to be the UK, but it has also received many positive hits in that regard, but not the most. In terms of our stolen travel document database, the UK downloads the information once a week and for stolen motor vehicles every night. In terms of our working group meetings, the UK always participates. The Metropolitan Police Department has put in place I-24/7, our communications system, and is sending an analyst. There are many areas where the UK is a leader, but the area in which I said Denmark is the best is in systematically sending us the fingerprints and the names of people who are arrested in Denmark, in order to determine whether or not they are wanted around the world. I have 182 member countries and they are all voting members, and so in my view they are all equal when it comes to the important role they play at Interpol.

Chairman: The lady sitting on your left unidentified is my predecessor as Chairman of this sub-committee, Lady Harris of Richmond, who has a brief question.

Q357 ***Baroness Harris of Richmond:*** It is a very brief question. Mr Noble, your written evidence fascinated me so much that I had to come along and see you for myself. My question is simply around the "arrested" bit of your evidence. Is it arrested or convicted? When you receive all the information on fingerprints and names, do you simply get it on people who have been arrested, who could then be proved to be entirely innocent, and then you retain that, or have they been convicted?

Mr Noble: I am embarrassed to say that when I became Secretary General I believed our files had the convictions of people. In fact, they do not have the convictions of people unless the convictions are related to the investigation. Interpol is an operational police support institution that helps member country police forces investigate people of interest to them. If they say, "Person X is of interest to us" and in the message they say, "He has committed three terrorist acts and we are worried about a fourth", then we would know that he had committed three terrorist acts, but the record of conviction is not in our files.

Convictions can be of interest to us and there seemed to me to be a void when the rapist murderer from France, who committed rapes and murders in Belgium, apparently was permitted to work in Belgium because the background check they did did not turn up that he had been convicted. Had they asked us about him, we perhaps would have said, "He is under investigation", but we would not have known whether he was convicted. In fact, going back to another question, we do not have a file of convictions unless it is related to an investigation that a member country is making about a person.

Q358 ***Earl of Listowel:*** How important is training in the development of an EU-wide counter-terrorism capability? What role does Interpol play in this area?
Mr Noble: Training is very important. It is an area in which we have been the weakest so far. We were fortunate enough to be invited to Bramshill to participate in a training course. We were so impressed that we asked Bramshill to send us two of their training course designers to come to Interpol. They met with all our senior staff. They designed a training strategy for Interpol that we have adopted in part; we could not adopt it fully because it was a bit too ambitious. We have created the post of Assistant Director for Training. We hope to have a much more robust training effort in the future than we have had so far. The number one request from member countries around the world we receive is to improve our training. When I met with Sir John Stevens Commissioner of the Metropolitan Police, he said the great difficulty for the UK is that if it receives a training request from a country, the FBI might receive a training request and the Australian Federal Police might receive a training request and they all go about providing training not knowing what the others are doing. The idea of having an entity where countries could send requests and offers of training would be something which Interpol could improve on and add value.

Q359 ***Earl of Listowel:*** In terms of exchanging personnel from one country to another in order to promote training and share capabilities in that fashion, are there limits on your resources that prevent you from assisting or is that something that you would like to assist with?
Mr Noble: Yes. We have 70 countries' police forces represented in our main office and in our regional offices. We believe that having a police officer coming to Interpol or going to one of our regional offices enhances his or her professional development and also provides the opportunity for him or her to give his or her country added value or support. We would like to be able to offer training at Interpol as the UK and other countries do. Yes, that would be something we would welcome.

Q360 ***Chairman:*** Mr Noble, thank you very much indeed. We are extremely grateful to you for coming here, as I said earlier, but also for the very full, frank and helpful answers that you have given to our questions. May I also thank Mr Williamson, from NCIS, your colleague behind you. I know you have a very tight timetable as you have a flight to catch this afternoon but I hope you will both come and join me for a quick lunch..
Mr Noble: My Lord Chairman, let me say, in closing, that it really has been an uplifting moment, not just for me but for my entire organisation, to be invited to provide evidence here. I can assure you that we will try to improve the services we provide to all our member countries. I would extend to each of you individually or collectively an offer to visit Interpol's General Secretariat in Lyon at any time that is convenient to you and we will try to show you first-hand what we do.

WEDNESDAY 8 DECEMBER 2004

Present	Avebury, L	Dubs, L
	Bonham-Carter of Yarnbury, B	Listowel, E
	Caithness, E	Ullswater, V
	Corbett of Castle Vale, L	Wright of Richmond, L (Chairman)

Memorandum by the Home Office

Justification

To a greater extent than ever before, terrorists have an international agenda and are able to operate internationally. To address this we need to ensure that co-operation with international partners is—and remains—effective. There are long-standing arrangements for close co-operation and information sharing between organisations involved in the fight against terrorism, both at national and international levels. These arrangements generally work well and are continuing to develop. While there are some areas where we would like to see more information made available, ensuring the quality, relevance, timeliness and appropriate protection of the information shared are also key concerns. Moreover, it is important to recognise that both privacy and national security considerations place some necessary limits on what information can be shared.

Data Exchange

The practical application of the principle of equivalent access to data by national law enforcement authorities in the EU as set out in the Communication from the Commission to the Council and the European Parliament (COM(2004) 429) is unclear. A large quantity of the data held by UK law enforcement authorities is tightly controlled even within the organisation concerned. This may be necessary for a variety of reasons, including privacy/data protection laws, national or personal security concerns, legal or ethical restrictions on the use to which information may be put, or the need to closely protect information during an investigation or pending a trial. Any requests for access to this information by EU law enforcement authorities would, accordingly, have to be considered on a case by case basis.

Where information held on UK databases is openly available to members of all the UK law enforcement authorities, it is likely that there would be no objection in principle to sharing this information with law enforcement authorities in other EU Member States. We would wish to get clarification of the Commission proposal before undertaking the further work needed to identify what information fell within this category and whether there would currently be legal or other constraints on sharing it with EU partners. The scoping study envisaged by the Commission should provide the clarification required.

Interoperability of EU Databases could be of benefit in a number of areas, including the detection of terrorists entering or leaving EU countries. Interoperability could take a number of forms. It need not involve giving open access to all (or any) of the information contained within the relevant database, though its benefits would probably be greatest where there was an agreement to pool or share a category of data. These benefits will, however, need to be weighed against the costs of creating common formats and any shortcoming in the common format itself from a national point of view.

Europol already holds centralised databases of police intelligence, and the feasibility of creating a forensics database is currently under consideration. The main drawback of a centralised database is that it relies upon all Member States supplying the relevant information, which in the case of Europol has been of variable quality and volume. Moreover, it will not be as up to date as national databases, due to delays in transmission (though interoperability could reduce these delays). Europol's databases are defined and operated under differing legal criteria in accordance with the Europol Convention. There would be considerable practical, resource and legal difficulties to overcome in managing a centralised database. However, centralised databases can offer an additional opportunity to discover links between terrorist suspects operating in different EU countries, especially where they are backed up by an effective analytic capability.

Data Protection

We do not envisage that there will be large scale increases in the collection and exchange of data as a result of the Commission proposals, or major changes in the nature of the information exchanged. The UK already has extensive bilateral arrangements in place with law enforcement authorities of other Member States to allow relevant information to be obtained where needed. We are also major contributors to the Europol law enforcement intelligence databases. The UK's current data protection legislation should, therefore, continue be sufficient. It would be for the Commission to establish that a common EU data protection legal framework, or common standards for the transfer of personal data to third countries/bodies, were necessary and proportionate. It is likely that reaching consensus on any such instruments would be difficult and time consuming.

The Role of the EU

Countering terrorism is a vital issue of national security which, in the new EU Constitutional Treaty, is defined as an essential state function to be respected by the Union. The role of the EU is thus one of support. However, there is a wide variation in the capacities of Member States to gather and analyse intelligence, and the terrorist threat is not confined by national borders. It has been agreed at Council that EU intelligence assessment needs should be met by establishing a CT Cell within the Situation Centre (SitCen), which operates within the Council Secretariat. In addition, Europol has been given extra resources to develop its existing CT workstreams. On the international front, the ability of the EU Member States to reach common positions on counter terrorism issues can add to the influence we are able to exert with third countries.

The Government does not believe that the EU has intelligence requirements which are distinct from those of its Member States. However, in agreeing community wide policies and legislation on counter terrorist measures, there is a need to reach a common view on aspects of the terrorist threat. EU institutions can therefore benefit from access to assessed intelligence material, but we do not believe that there is a need for "an EU intelligence policy".

There is a high degree of consensus among EU Member States on counter terrorism issues. This was demonstrated, for example, in the Declaration on Combating Terrorism agreed following the Madrid bombings, where the EU did speak with "one voice" and expressed its solidarity with Spain. It is obviously important that all EU member States are committed to fighting terrorism, that they have effective CT arrangements in place, and that they co-operate with each other and with other international partners where necessary. However, uniformity is not required, and national approaches will sometimes differ. The EU must respect the differing legal and constitutional traditions of its Member States.

There are a number of informal groupings within the EU at which policy issues, including counter terrorism, are discussed. As well as the G5 these include the Salzburg Group (Austria, Poland, Czech Republic, Hungary, Slovakia and Slovenia), the Benelux countries, and the Baltic Sea Task Force. Such groupings can assist rather than hinder the development of EU wide initiatives, allowing Ministers to discuss informally matters of particular importance to their countries, and enabling a freer exchange of views and ideas than would be possible at formal EU Meetings involving all 25 Member States.

Institutional Arrangements

Counter Terrorist activity within the EU is currently dispersed between a large number of different committees dealing with areas such as immigration, borders, transport, criminal law, police co-operation, and foreign policy—as well as those dealing with terrorism itself. There is a need for someone to maintain an overview of this activity, to ensure that there are no gaps or inconsistencies, and to report on progress. The Government believes that this, together with an examination of effectiveness of EU structures in delivering the counter terrorism Action Plan, should be the focus of the new Counter Terrorism Co-ordinator work, rather than policy development or international representation.

The Government would like to see some rationalisation of EU committees dealing with terrorism. We feel that, at present there is some overlap between the roles of the existing committees, while arrangements for dealing with cross pillar, policy issues such as terrorist finance and radicalisation and recruitment are inadequate. The Government believes that Europol should concentrate on the analysis of criminal intelligence in support of law enforcement agencies in Member States. We do not see a useful independent operational role for Europol in fighting terrorism within the EU.

Training at EU level provides a hands on way of sharing experience and good practice between Member States. CEPOL, although only in its third year of operation, is now well-placed to contribute to the coordination and benchmarking of EU police training. The Secretariat is permanently established at

Bramshill and will soon have legal personality and be properly resourced. This will enable it to deliver its ambitious training programme for 2005, which will contain 51 modules covering 30 subject areas, including counter-terrorism, setting up joint investigation teams and intelligence-led policing. It will be delivered through a network of national colleges. Around 870 senior police officers (up from 500 in 2002) received training in 2003. There is also a growing emphasis on co-operation with Europol, training trainers, and developing the research database. Furthermore CEPOL can contribute to furthering EU (and thereby UK) links to Third Countries in the Balkans and the Mediterranean. For example, the MEDA programme involves 12 countries—Algeria, Cyprus, Egypt, Israel, Jordan, Lebanon, Malta, Morocco, Palestinian Authority, Syria, Tunisia and Turkey. It is a two year project costing €2m, and is designed to provide training for trainers in money laundering, anti-terrorism, drugs, and organised crime linked to new technologies.

David Blunkett
Home Secretary

9 September 2004

Examination of Witnesses

Witnesses: Ms Hazel Blears, a Member of the House of Commons, Minister of State, Home Office, Mr Bob Whalley, Director, Crime Reduction and Community Safety Group, and Mr David Makinson, Crime Reduction and Community Safety Group, examined.

Q361 ***Chairman:*** Minister, welcome. Thank you very much for coming to give evidence today. Can I also thank you for the Home Secretary's letter which is very useful evidence for us. Could I ask you to introduce your colleagues?
Ms Blears: Certainly. On my right is Bob Whalley.
Mr Whalley: I have the post of director for counter-terrorism and intelligence in the Home Office.
Ms Blears: On my left is David Makinson.
Mr Makinson: I work in the Crime Reduction and Community Safety Group on international cooperation.

Q362 ***Chairman:*** Can I first register the subject of the inquiry? It is an examination of a number of proposals designed to strengthen EU counter-terrorism activities, particularly through much more extensive data exchange. These proposals raise important issues relating to, among other things, data protection and the institutional arrangements within the EU for combating terrorism. I will not ask Members of the Committee to register their interests because they have already been registered and are at the back of the room, I am told, if anybody wants to consult them. Minister, would you like to make an opening statement?
Ms Blears: Yes. I think this is a very important inquiry and the range of issues that have been raised in the questions is the right area to probe and inquire into. I hope our discussion today will be very useful and worthwhile. I hope it will assist me as well as, hopefully, assisting the Committee. I want to set out very briefly what our priorities are in working with the European Union on the counter-terrorism agenda. First of all, to try and make sure we have an effective, coordinated response not only to what happened in Madrid but also to the continuing threat that we face; that we retain our ability to act flexibly and to respond to the level of threat that is clearly out there; that we have a real sense of a multidisciplinary approach. The fact that these issues cross all three Pillars of the European Union is a particular challenge for us. Therefore, the role of coordination and integration is particularly key. My overriding aim is a very practical one, to make it harder for terrorists to operate within the European Union, to make it the most hostile environment that we can for terrorists across a whole range of issues. We want to deliver that through not simply what we do in the European Union but also through our foreign policy in terms of the Second Pillar of our operation, to try and make sure that we do very practical things about undermining terrorist financing and the increasing use of identity fraud which underpins terrorist activity, to make sure that we maximise the use of technology, not only in border security but in detection. There our Project Cyclamen is particularly important for us, to ensure that counter-terrorism issues are integrated across the machinery of the EU and to try and make sure that we make the best use of Europol. Their capacity has been strengthened and there are more resources going into Europol. I think it is incumbent on us to get the best value out of that. My overriding message here is let us do things together where it gives us added value in our efforts in this country. I genuinely believe that working with the European Union in a constructive way can give us added value. One note of caution: we do not want to get too tied up in the machinery which could affect our operational ability to be out there, fighting terrorism.

Q363 ***Chairman:*** Thank you very much. The last point you made is very much in line with the Home Secretary's remark that he sees the role of the EU as very much one of support to Member States. Do you

think there is a risk that current developments might undermine this degree of support as more work is undertaken at EU level? In other words, is there a risk of undermining the role of Member States?
Ms Blears: No. I think it is a matter of getting the balance right. The European Union action plan which is very comprehensive and very detailed is of great help to us in concentrating and focusing our activity. It certainly raises the issues right across the 25 Member States. The UK is at the leading edge of implementing a change. We certainly do not feel threatened or undermined by EU activity because we are major players in that very activity, but it is important for us to stress that we think EU activity should be adding value to the work of Member States. There are areas where those links can make a real contribution, whether terrorist financing or identity fraud. The links with organised crime are absolutely key for us. On 17 December there will be an update. There has been significant progress reported on intelligence cooperation, exchange of information, civil protection and around consequence management planning as well, which is a very important part of our contest strategy and clearly it has some European Union implications too. The fact that there is a regular review of progress is really important. When we take over the presidency, we will be having our own review towards the end of next year. I think we have sufficient mechanisms to ensure that the thrust of adding value is not undermined by the closer integration at EU level.

Q364 ***Chairman:*** You referred to the role of Europol and I think we will pursue that later on and possibly cover Interpol as well. I wanted to ask about the European Police Chiefs Task Force because the European Council declaration of 25 March this year underlined the role of the Task Force in coordinating operational responses to terrorism. Our impression is that it has not been terribly effective so far. Do you agree with that? If so, why do you think that is?
Ms Blears: I certainly do not think it is down to any lack of dedication and enthusiasm on the part of the Task Force. They have really wanted to do the job that has been set out for them. They have found it difficult because they have not been passed the formal structures of the European Union. They were not set up in a formal way. Their lack of access particularly to the Article 36 Committee has perhaps hindered them in making the impact we would want them to. They have two roles in terms of a strategic role around setting a framework and sharing best practice and they also have a very important operational role about coming together and planning joint operations. Now the situation which has been agreed, as I understand it, is that they will meet occasionally with the Article 36 Committee. That will give them that added impetus and strength in the role they can play.

Q365 ***Chairman:*** You do not think there is more that we ought to be doing on this at the moment?
Ms Blears: They need to be more closely connected in order to have more influence. What is proposed at the moment is let us try that and see if it does give them the impact that we want to see before taking any further steps. If they are well linked in to the Article 36 Committee and get that high level discussion, that will help them. We in this country play a significant, major role in that European Task Force of police chiefs and we have a lot to offer in trying to make it a more effective group.

Q366 ***Viscount Ullswater:*** Why do you think the Police Chiefs Task Force was set up on that sort of basis if it seems so evident both to you and from the evidence we have heard in Europe itself that there was this slightly structural difference because it was not set up under an EU structure? It does not seem to fit in. Why do you think it was set up like that?
Ms Blears: I do not know. Perhaps Bob is able to help you in this area.
Mr Whalley: I cannot offer you much on that. It goes back four or five years now and you can see the desire to give some sort of operational linkage. All these organisations respect the operational independence of chief officers and that is obviously important but equally, if we are going to have a comprehensive EU approach, there comes a time when there has to be some linkage with the formal structures. Maybe it is simply a process of evolution which has brought us to that point.

Q367 ***Chairman:*** Am I right in thinking that this originated from the Tampere Council and a British suggestion?
Mr Whalley: Yes, to promote better coordination in an operational sense. That is important but now experience has shown it may benefit from being linked in with a structure, particularly with a senior, civil body such as the Article 36 Committee.

Q368 ***Lord Dubs:*** The National Crime Squad has supported proposals to establish small operational teams made up of interested EU Member States and they should take forward intelligence-led operations. Do you think this is a sensible way forward? Might it lead over time to the EU developing an operational capability?
Ms Blears: First of all, do I think it is important that there are small teams with operational activity? Yes, I do. This has gone on for many years where there have been matters of interest to several Member States in terms of cross-border crime, serious and organised crime and the links to the terrorist agenda. It is very

important that those kinds of operations take place. The second part is developing intelligence-led joint operations and we are very keen on intelligence-led policing, not just in this country but also in the European context, which is why we are pushing so hard for people to start to develop perhaps a European model of our national intelligence model that we use in this country. Intelligence-led operations are absolutely key. Joint operations between interested Member States are important but I do not think that what we want is European Union operational capacity of its own accord with law enforcement officers in one state having powers automatically in another state, where we will begin to see an overlay of European Union competence rather than Member States competence. There is quite an important distinction for me between people coming together, cooperating on an issue that threatens their individual Member State's interest and making sure that the law enforcement officers have intelligence, information, operational capacity to deal with that. That is a world apart, for me, from having a system of law enforcement that has automatic competence to take action in other Member States and I really want to make that clear.

Q369 ***Lord Dubs:*** Do you think we have the balance right between focusing on tackling terrorism within the EU compared to on a global basis? I looked with interest at the Home Secretary's letter and he was a little bit sceptical about some aspects of Europol operations. I just wondered whether we have the balance right between supporting Europol and working in that way and giving more back to Interpol.
Ms Blears: I think you are right to ask if we have the balance right. It is not a matter of doing one or the other. It is absolutely vital that we do both. There has been an acknowledgement from the EU in terms of the declaration at the Council and the action plan for Madrid that we face a terrorist threat both from within the European Union and clearly it is a global phenomenon and we face the threat from outside as well. We have to make sure that we strike that balance according to the threat and according to the institutions with which we are properly connected in Europe. That is why we do want to play a major role in making sure that the European machinery and institutions are effective in tackling the counter-terrorism threat. We are playing that role and we are committed to doing that but equally, in terms of the global threat, the work that has been done through the G8 and the European Union in terms of our work with third countries, it is absolutely key to this. It is not a matter of us facing inwards and simply looking at what happens in the EU. We are using our EU structures to enable us effectively to engage with those third countries from which the threat also emanates. I think we have the balance right in terms of our political priorities, which are that we do both. We have quite a lot more to do in terms of removing some of the barriers there are to information sharing, to sharing intelligence and making sure we have the right intelligence products to enable us to tackle these issues. I do think we are trying to work on both these issues as effectively as we can.

Q370 ***Chairman:*** You referred to the role that we are taking in this. Have you or your colleagues any comments to make on the new members of the EU and how far they are yet operating effectively in the counter-terrorism field?
Mr Whalley: I do not have very much on that, no. We have worked for some time with the 15 and we have worked for many years with those countries that are about to join. It is going to be quite a challenge to get a commonality of approach and purpose across 25 countries. They have very different legal systems and a very different approach to these issues. There will be a determination among all of them to deal with the terrorist threat. I think we shall use the opportunity of our presidency to get best practice, common standards and all the work that needs to be done on legislation, for example, promoted across the 25.
Ms Blears: We are doing a lot more with Interpol than has previously happened. Interpol has such a wide reach into 181 different countries. It is important that we harness that capacity to help us work within the European Union and one of the things that has happened most recently is that we have agreed that the information that Interpol has on lost and stolen passports can be passed through to Europol so that we have an exchange of information in that way. I would not want you to think that Interpol is over here and Europol is over here and there is not really good dialogue between the two.

Q371 ***Lord Dubs:*** I am delighted to hear what you say about Interpol. We had the head of Interpol giving evidence last week. Apart from being very impressive in the way he gave his evidence, he also left me—and I think all of us—with the impression that Interpol was the poor cousin in its relationship with Europol and Interpol was not getting the sort of support that Europol was getting from countries as a whole. He also made one specific comment. He could not understand why our landing cards for foreigners coming into the country do not ask for passport numbers, particularly since in every known case of terrorism fraudulent use of passports was a feature. It may be unfair to lob such a specific question at you but I wonder whether I can leave the question with you and maybe Mr Whalley or Mr Makinson could come back to us. On the general question of the balance between support for Interpol and Europol, I must say we were left with the very clear sense that

Interpol felt they were being a bit left out in the cold on some things.
Ms Blears: I will reflect on that and get back to you on the specifics. We were aware of it and we have been thinking about why that did not happen. I am concerned if Interpol feels they do not have that kind of support because the facilities they offer in terms of their 24 hour reporting system and their work with various countries are very important to us.

Q372 ***Lord Avebury:*** You said that Interpol data on lost and stolen passports would be passed back to Europol. Has it not been agreed that when Member States receive details of lost and stolen passports they will notify them simultaneously to Europol and Interpol and in those circumstances what is the point of keeping a Europol database of lost and stolen passports at all, because it will only be a subset of those which are held on the Interpol database which includes those from other parts of the world not included in the EU?
Ms Blears: I suppose that may be the case when it works perfectly, but we do not want duplicate information, clearly. Many of the questions that your Lordships have raised are about effective exchange of information and the interface of databases. I would hope your Lordships would agree with me that exchange of information does not happen perfectly in the first instance. It is a developing area and it may well be that we need to keep some of the information for a period.
Mr Makinson: The value of the Europol work is more on the analytical side. It is not just about a database of the numbers of stolen passports. It is more that they look at countries from which they have been produced and all the strategic matters surrounding the issue, rather than it just being a check list. Interpol will provide a very useful service in that regard, but Europol's work is slightly different.

Q373 ***Lord Avebury:*** As long as Europol have access to the Interpol data, there is not any purpose to be served by having them own a separate copy of the data. They can undertake the analytical work that you mention without physically owning the data.
Mr Makinson: That is true but they need to have it in the first place to do the analytical work. I cannot see a way around that if Europol is to provide added value on the issue of lost and stolen passports.

Q374 ***Chairman:*** Incidentally, one of the points that Mr Noble made to us was that Interpol are particularly able to help with fingerprinting records. I happened coincidentally to see in the press on the following day that our fingerprinting computers had broken down. Have you any comments on the computerisation problems of exchanging this sort of information?
Ms Blears: The robustness of our information technology systems is as good as we can make but I do not think anybody dealing with major databases in any aspect, not just of government but also the private sector as well, would say those systems work 100 per cent every single day and hour of the year. There are breakdowns and it is necessary to reboot systems and get them working again. There was a breakdown of the automated fingerprint service and we got that back on stream as quickly as we could. It is a tremendous development from where we were in doing manual searches for fingerprints. Although it may be subject to breakdown from time to time, the step change it has delivered in our ability to get identity information very quickly should not be under-estimated. There was a similar incident in the Department for Work and Pensions a few weeks ago when many of the screens went blank and had to be rebooted very quickly. When we come to some of the later questions on databases, I feel we will have a concern about the cost benefit analysis in terms of making sure that these things fit together.
Chairman: Lord Caithness will remember 15 years ago I was sitting where you are sitting, in front of the Public Accounts Committee to try to explain why the Foreign Office's information technology had broken down.

Q375 ***Lord Corbett of Castle Vale:*** You say that you do not envisage that there will be any large scale increases in the collection and exchange of data as a result of proposals from the Commission and the Swedish Government but does not the idea of equivalent access and the principle of availability presuppose greater sharing of information?
Ms Blears: Yes. I have been thinking carefully about what is equivalent access to data; what is the principle of availability? Are they the same thing? Are they two ways of expressing the same thing? Are there subtle differences between the two in terms of the practical implications they will mean for us? There are some differences. When we say we do not think it will mean us having to collect or share more data, that is because the principle of equivalent access is about access to data which already exists. Secondly, we share a huge amount of data in this country. We contribute something like 40 per cent of the data that goes out. What we would be looking for is some advantage in this better exchange of data in that as a country we would have access to more data than we currently have. If people were to do the same amount of sharing as we do, that pool of data would be significantly larger than it currently is. That would be an advantage to us rather than a burden. In terms of the two principles set out so far currently being discussed by the Commission, the right of equivalent access is about criminal intelligence information that is out there being shared. That is a wider definition.

You have the information. There should be access for people in Member States to that information. When you come to the principle of availability, that covers not just criminal intelligence but also security service intelligence. In that area, we do need more safeguards, more conditions, more case by case analysis on how that can be shared. That is envisaged by the proposal that has been put forward which sets out for the principle of availability a number of checks in the system. We do not see this as being a bigger burden to us. We want to take it step by step and cautiously because it could have an impact, particularly on our security service information.

Q376 ***Lord Corbett of Castle Vale:*** You have repeated what is also said in the Home Secretary's letter about deciding this on a case by case basis. Does that not collide with what the whole purpose of this exchange is about or are you saying that if we treat this like a layer cake you decide which information goes where on the basis of who you want to have access to it? Is that what you mean by a case by case basis?
Ms Blears: Yes. I would not say that this collides. There is a tension there but I do not think it is a mutual exclusivity. I do not think it is either you have a principle of availability or you have to examine each and every single request. There are some sectors of information where you could have broader access, particularly around criminal intelligence where we want to share the cross-border crime and the operational requirements that we have, but you become more selective as that information gets more sensitive and you have more case by case examination on that spectrum, as some of the information strays into fields that you would have some genuine concerns about sharing on a multilateral basis. You might have less concern about sharing it on a bilateral basis because that has always happened, but we are talking here about multilateral information sharing.

Q377 ***Viscount Ullswater:*** Minister, if I could take you on to the databases themselves, you mentioned in a previous comment about the exchange of data interoperability. You probably see some benefit in interoperability of EU databases but you have already mentioned the cost benefit analysis that needs to go on. How practical would you think this would be with the existing databases?
Ms Blears: "Interoperability" is a horrible word. I am convinced now it is a real word, which I was not initially. Where there are some existing common platforms for databases, it is easier to do. The European visa information system and the Schengen information system too share the same technical platform. In practical terms, it will be easier to plug those types of databases together and it is useful to know that somebody has applied for asylum in two different Member States and been refused on grounds of national security. If I think about some of the different databases in different Member States—for example, our police national computer together with all the police national computers of all the other Member States—and I think about translating it into lots of different languages, different standards of information, I would want a proper analysis of what the benefits are from having that interoperability and what the costs are in terms of having that access. There are clearly data protection issues and the bringing together of the data protection rules around that. These are quite complex issues. When you have common platforms and you share biometric data and it can be brought together easily and simply, that can have some tremendous benefits for us. Perhaps where you have some conviction data where somebody is convicted of a sexual offence perhaps in one country, you could share that information and that could help you in pursuing a prosecution and investigation of that person. There are opportunities out there for us but I do not think interoperability of databases is a panacea for necessarily making us more effective.

Q378 ***Viscount Ullswater:*** We visited the Immigration Department and we were shown the fingerprinting which I think is now on Eurodac. That seems to be the interoperability that could be a common format but obviously if you are going to go further than that you see there is quite a disadvantage about trying to reduce everything to a format. There may be some shortcomings I having a format which is interoperable.
Ms Blears: We are facing these issues in the national context as well as an international context. We have the Bichard inquiry looking at how our police forces in this country share or do not share their intelligence information and making sure that we can protect people in those circumstances. These are issues facing every Member State and facing us collectively as the European Union. I have a healthy degree of scepticism about this area. Where we can use technology to bring our information together and to make us more effective, we should do that. I also want to be convinced that going down this path is not simply seen as an easy option because there are quite a lot of hurdles in terms of common format, common language, common supervisory systems, common access, common privacy safeguards. It is not simply saying, "Would it not be marvellous if we all had a massive European Union database that told us everything about everybody that we wanted to know?" I know that is a simplification and I do not want to parody what people have put forward, but I think it is a genuine attempt to have a bit of rigour into where it is appropriate, where we can do it, where we have the technical competence and expertise,

where we have Eurodac, the visa information system and Schengen coming together. That seems like a really good idea but I need to be convinced that the same considerations apply necessarily to all the individual Member States' own particular databases in different areas.

Q379 ***Viscount Ullswater:*** Both the National Crime Squad and the NCIS see a case for a centralised EU database for law enforcement purposes. I think the government have explained they see drawbacks to it, particularly in terms of Member States not supplying information fully and promptly. Do you think we ought to work on these difficulties and overcome them or do you again have a little scepticism?
Ms Blears: I am also an optimist. I think we should work together to try to ensure that we are as effective as we possibly can be in sharing information for the purposes of fighting crime and combating the threat of terrorism. If you look at some of the common factors in terrorism, they are around identity, finance and the interface with serious and organised crime. Therefore, there is nothing more important to the wellbeing of this country than that we use every single tool we can to make sure we are as best prepared to combat that threat and to pursue terrorists as we possibly can be. I think we should put effort into making sure that we are as strong as we can be in this field. I want to make sure that it is effort well spent in terms of getting the results in coming together with our information systems.
Mr Whalley: The point here is that we have a lot of databases. Obviously we need to make sure we get the full benefit of those before we think about how much we could do from a centralised one. When we get the existing databases communicating with one another the national organisations can get access to them when they need to and that will give you more evidence as to whether you needed to build something else.

Q380 ***Lord Avebury:*** The Home Secretary told us that reaching consensus on instruments for data protection for the third pillar is difficult and time consuming. Considering we already have such a system in the First Pillar, why do you say that?
Ms Blears: Because 23 of the 25 Member States have already translated the First Pillar Common Directive and have a system that applies to law enforcement provisions. The other two states also have law enforcement specific provisions around data protection in their countries too. I am not clear. It takes me back to the very beginning of this session as to whether or not a new European Union wide regime is strictly necessary if the provisions that accord with that First Pillar have been enacted and the Member States already have sufficient schemes in place themselves. The question I would ask is what is the necessity for having either an additional scheme or something that is decided centrally that is then superimposed on the Member States' own systems. I am not clear what added value would be brought by having a European wide supervisory system here. We should be doing things on a European Union wide basis where it adds value and I have not seen any strong arguments as yet that a new European wide system would bring that added benefit.

Q381 ***Lord Avebury:*** The question whether there should be a European wide supervisory system is separate from the question whether or not there should be a data protection framework for the Third Pillar. Do you think it makes sense to have four separate supervisory bodies?
Ms Blears: There might be some benefits in bringing the supervisory regimes together. I am sure that is something that will be explored. It is important that we are assured that the data that is exchanged is used for legitimate purposes between us. It is quite a sensitive area for many people that we get broad consent to people to exchange information, provided people are reassured that that information is used properly, legitimately and for the purposes for which it was requested. The whole function of our data protection regime in this country is to get that balance right between the needs of security and the needs of privacy and safeguards. This is a very delicate political balance and becoming more so as technology develops and the proliferation of information develops. It is a careful line to tread to make sure that we reassure people that our data protection regimes are robust enough to allow them to have trust in giving us access to more information. That is why I think the transfer of data has to be protected but there might be benefits in bringing together the various supervisory regimes so that people are clearer about what the standards are in terms of those safeguards for their privacy and protection.

Q382 ***Lord Avebury:*** You do not envisage that the UK would have any definite proposals to make on bringing together the supervisory regimes during its presidency of the European Union?
Mr Whalley: We will look at anything which would help to promote better coordination here. We have to recognise the principle here. We are talking about the difference between the First Pillar measure and the Third Pillar measure. There are areas which are in the First Pillar and areas which are in the Third Pillar. It would be quite a step to move to having a data protection regime in the Third Pillar which was out of line with the fact that the Third Pillar measures are within national competence, which would bring me back to the regime: what does each Member State have by way of data protection requirements in the

Third Pillar. Those are the requirements which Member States will expect to adhere to in following through a Third Pillar measure.

Q383 ***Lord Avebury:*** Is it not going to be very cumbersome if you rely on the data protection regimes within each Member State and, as the Minister has said, you believe in equivalent access and interoperability as far as the factual databases are concerned? Those, for example, deal with biometric data or convictions as opposed to those which are more subjective and vary between Member States according to the legal systems they have. If you are going to have this greater degree of interoperability and equivalent access on the factual databases, would you not have to have individual checks for each of the 25 member countries if you do not have a common Third Pillar data protection framework?

Ms Blears: You either view this as an area in which you have a kind of big bang approach and you go for a belt and braces approach on interoperability, sharing everything and having a regime that covers the whole thing. That may be a legitimate approach. It certainly is not the government's approach. What we want to adopt on the data protection regime, similar to interoperability, is what do we have that works and that is the most effective, practical way we can do this. If we can do it within our existing system, we do not want to simply set up supervisory regimes and data protection regimes that could lead us to have a more complex system unless it is necessary. I want to take it in that kind of layer approach which I think Lord Corbett talked about of what is necessary in relation to what has been requested, what is the purpose, how can we bring it together and what are the necessary safeguards in that system to enable us to have access to it.

Mr Whalley: Obviously, it is very important to promote better cooperation and exchange of information but I do not think we would be the only Member State which would have some difficulty in going forward for some sort of data protection regime which went further than the regimes within national competence. This is an issue where we should work towards finding what are the common standards and baselines and practice that we can all build upon. If the Community as a whole is keeping these issues in the Third Pillar, there would be quite a significant challenge in building in a data protection regime which was not aligned with the Third Pillar competence.

Q384 ***Earl of Caithness:*** Are you satisfied with Europol's work so far and the work that is done in relation to the Management Statement?

Ms Blears: Yes. We feel that Europol is playing a very important and full part in trying to complement the work of the Situation Centre on counter-terrorism and the fact that the national liaison officers from Europol can come together and work together is particularly important. I do not think it needs more powers at the moment. It needs to make sure that it uses its increased capacity to best effect and that is where I want it to be focusing and to be thinking particularly about terrorist financing, the identity fraud and the interface with serious and organised crime. Its analysis that it can do where it has been able to throw up links between individual terrorists or cells that are operating out there and its work on financing is particularly useful for us. We are quite happy for Europol to carry on working in the way it is. What I would not want it to do is duplicate the work that is going on in Member States in other areas. I would not want it to be so ambitious that it spreads what are still limited resources too thinly and did not work to best effect.

Q385 ***Earl of Caithness:*** Given that in the Home Secretary's letter extra resources have been given to Europol, could you tell us what those extra resources are and how are you going to prevent Europol creeping upwards and duplicating what other agencies are doing?

Ms Blears: I do not have the detail of the extra resources but I would be more than happy to write and set those out. My understanding is that their particular added value role is around analysis. I would expect that some of those resources are being directed into analytical capability. That is where we would want them to try and concentrate their work. We also want to try to promote the idea of a European wide criminal intelligence model where we see Europol increasingly providing intelligence product, contributing to the threat assessment and that kind of work at that level. In terms of what levers we might have to prevent their mission creep, I am not sure that we can directly direct them.

Mr Whalley: It is a very important issue because we do not want Europol to develop a mission creep. We would like it to do the things it is supposed to be doing. It is a very similar issue to the one about the Police Chiefs Task Force. It is making sure that operational independence is preserved but that Member States keep a reasonable overview and control over what is going on. I would hope that we can align what Europol is doing more clearly with the ambitions of the Union as a whole. It seems to me it should not be a separate agenda; it should be working to support what we want the EU to develop and deliver. That is the thrust of it and we will look at this during our presidency.

Q386 ***Earl of Caithness:*** Thank you for undertaking to send us that extra information and when you do could you also let us know how you are going to make certain that that money and extra resources have been spent wisely and cost effectively?
Ms Blears: Indeed.

Q387 ***Earl of Caithness:*** Another area where there seems to be a creeping of Commission ambition, for want of a better word, is the EU intelligence policy. There is a Situation Centre. You are establishing a new CT cell within it and the Commission are longing to have an intelligence policy, but the Home Secretary is saying he does not think that is the right way to go. Who is going to win this battle?
Ms Blears: I would not characterise it as a battle. It is a robust discussion and it brings back to getting the balance right because we do want increased cooperation, information sharing and we want to make ourselves as effective as we can be in fighting the terrorist threat. In terms of an intelligence policy, what we do not want is an origination of intelligence at European Union level. We want a drawing together of the intelligence that is collated from Member States' own intelligence capabilities. The added value from that is the analysis that we can bring from having brought together all those sources of intelligence and then come up with extra information that will help us in terms of combating this threat. We have to be careful to avoid European wide institutions wanting to create something fresh that comes from simply a European perspective rather than necessarily a bringing together of the information, skills and expertise that Member States have to offer. We think there should be a common intelligence policy in terms of sharing particularly the criminal intelligence that we have on these people who operate across all our Member States. What we do not want to see is an origination where people are seeking something entirely different and divorced from the effort that Member States may have developed. It is a distinction but certainly not a battle.

Q388 ***Earl of Caithness:*** Your concerns are equally shared by Mr Noble of Europol who rather believes that the EU's answer to any problem is to set up another policy area and another unit to deal with something instead of using the existing structures better. Can you give us a sketch of what the other Member States feel about this issue? We are very clear about where the British government is. What about the French, German, Italian and Spanish governments on the issue of EU intelligence policy?
Mr Whalley: I cannot give you a precise answer on that. From the meetings that the Home Secretary has had with his colleagues in the G5, there is a pretty clear recognition that we do not want to be setting up more bodies. It is a question of making better use. We have to bear in mind two things. One, in this country, we are quite well served in the intelligence flows which we have and we have a very close linkage between the intelligence community and the civil machinery of ministers. That is not the case in every Member State. Of course, many of the new Member States do not have the facilities that we have and equally after the Madrid bombings in particular there was quite a discernible surge within the Member States to have better information and to provide a better analysis of the terrorist threat. That is in our interest. We should make sure that the terrorist threat is well understood throughout Europe and we can contribute to that. At that level of building understanding, there is a value here.

Q389 ***Lord Avebury:*** Yesterday, when President Musharraf was addressing a meeting in room 14, he referred very frankly to what is taught in some of the Madrasas and the way in which people are being incited to religious hatred, which is one of the bases for terrorist recruitment. Do you think Europe should have a common intelligence capability for monitoring what is said from the pulpit in countries such as Pakistan, Bangladesh and Indonesia?
Ms Blears: These are hugely controversial issues, as you know from the Second Reading of the Serious and Organised Crime bill that we had yesterday and the amount of debate there was on the proposal to introduce the new offence of incitement to religious hatred. Clearly it is a matter of concern that people should not be allowed to incite hatred of other people on the grounds of their religious beliefs. Because we have this concern, we are proposing to legislate on it. That will be very controversial indeed but the intelligence that we need to collect should not simply be about that issue. I think there is a requirement on us to do much more around the prevention agenda, around the radicalisation, around the factors that lead particularly to young people feeling alienated and possibly being driven into the arms of terrorists. I am conscious of that in our own UK strategy and one of the elements of our contra-strategy is the prevention strand. Internationally as well we need to do more in terms of focusing on the reasons for radicalisation and what measures we can introduce together to try and combat that. I would not single out religious hatred here but the issue of radicalisation is very important.

Q390 ***Earl of Caithness:*** Moving on to the counter-terrorism coordinator in the EU, what contribution and added value do you think he has brought to this difficult area? Do you think he is heading in the right direction or is he heading too much towards policy development rather than getting a balance?

Ms Blears: First of all, I think he has a pretty awesome task in being charged with coordinating the European Union's structures, institutions and the ways of working around counter-terrorism. It is a task that needs doing and he has been very influential in drawing up the action plan which is very comprehensive indeed in terms of the work streams that need to be brought together. He has brought out an increased focus on this work and to try and make sure he works across all the Pillars to draw together the counter-terrorism work is very important indeed. I think he is doing that job very well. For example, the work around terrorist financing where we have done work on charities, on freezing the assets of terrorist organisations. I think it would have been quite difficult to get that kind of work done across those different strands of EU work without having somebody charged with that coordination role. My one serious point was that the coordinator does need to concentrate on delivery of the action plan, making a difference, getting things done and that takes me back to my original remarks that my focus is making sure that the European Union is a hostile place for terrorist activity. I want to see that action plan being chased and driven and really pushed across Member State. I think that is the priority for the coordinator's work rather than new policy development, but actual delivery of the things that have been agreed.

Q391 ***Earl of Caithness:*** In our presidency are you going to be pushing hard on that?
Ms Blears: Yes, we will. It is a priority for us and it is an excellent opportunity in our presidency to make sure we drive that action plan forward working with the European coordinator.
Mr Whalley: We have been very active in engaging with Mr de Vries since he was appointed. We have seen him. We have invited him here several times. We keep in close touch with him. We have made all the points to him which the Minister has made. There is a serious job to do here and we would expect to see some progress before our presidency and we shall make sure we follow that through in our presidency.

Q392 ***Baroness Bonham-Carter of Yarnbury:*** The other thing you mentioned in your opening remarks was the desire to do things together when it is providing added value. Specifically you say that the government would like to see some rationalisation of EU committees dealing with terrorism. How would you like to see the present arrangements streamlined?
Ms Blears: It is currently spread across all three Pillars of the European Union. It is important that the machinery works well. We had the discussion about the European Police Chiefs Task Force and the fact that they were outside the machinery which meant perhaps they were not having as much impact as they could do. It is my understanding that the counter-terrorism coordinator, Mr de Vries, was charged with looking at the European Union committee structure and there were three distinct options put forward as a result of his work. We could have a merger of the foreign policy group with the home affairs group. The second option was to create a new director level committee to oversee the two committees currently going on. The third option was to use COREPER and the public representatives' committee to coordinate this work. It was the last of those options that was agreed. We did support that because we did not want to see the new machinery brought in. Where we are now is that we want to see how that works in practice. Rather than having any more immediate changes in machinery, we would want to see that group at that very high level can bring some clarity to the way in which we organise our business.

Q393 ***Chairman:*** The Home Secretary's letter refers to informal groupings within the EU. I am grateful to him because he has drawn my attention to something I did not know before and that is that there is a Salzburg group and a Baltic Sea task force. As far as the G5 are concerned, we are conscious of some resistance within the Commission to the idea of these informal groupings. I see that the Home Secretary says that they can assist rather than hinder EU wide work. Have you any comment on the Commission's attitude? I suppose it is fairly predictable. They think all this work should involve all 25 rather than groups getting together. Have you anything you want to add on that?
Ms Blears: I do not think it is a case of groups coming together to undermine the wider EU effort. Inevitably on issues like this you will have some Member States that are perhaps more focused and more engaged and a little ahead in terms of the practical action they can take. Far from undermining the EU effort, quite often if you get a group together you can make some progress, for example, on forensics, on sharing information that you have and they can be used as an example of best practice. They can help to drive the rest of the policy. They can help people who are not as focused or, if we are honest, do not necessarily have the resources to be able to take that initial action. I want the Commission to be more confident when people get together that it is not about undermining collective action; it is about trying to make progress a little more quickly. With 25 Member States now, I think it would be wrong for us to make progress at the speed of the slowest on every area.

Q394 ***Chairman:*** Is there any institutionalised arrangement for the groups to communicate between each other and for them to report to the 25 on the outcome of their deliberations?

Mr Whalley: It is very informal. It is up to the country which is holding the informal chairmanship of the G5 to do that. While we had it, we did take steps to brief the Commission and the Dutch presidency. We wanted to make sure they were aware of what was going on. Your point is absolutely right. The country doing it must make sure that the presidency and the Commission are fully briefed. If I think back, for example, to the last G5 meeting which the Italians chaired, all the interior ministers had a discussion about what they wanted Europe to do. They looked ahead at the radicalisation agenda and the issues Lord Avebury has been raising and they decided they wanted to do more on terrorist financing. There I saw three very specific outcomes generated with some power and vigour by five senior Member States and it seems to me those are the sorts of issues which should be taken forward in the Commission. It does not need to be in a threatening way. It can add value to what the Commission are doing.

Q395 ***Viscount Ullswater:*** What I am gathering from your comments is something slightly different in that the structure of the EU now with 25 is not going to be able to be radical enough without these small groups. Are you saying that?
Mr Whalley: I do not think I am saying it will not be radical enough. The Home Secretary takes the view I think that those Member States that have these particular problems such as counter-terrorism and have some influence in resources should make sure they are pulling in the right direction and, if necessary, helping to bring some of the other Member States along. If it is handled sensitively, I do not believe it need be a threat. It can be used to help particularly those countries that have just joined, who are not fully aware of what the potential is of all the machinery we have there.

Q396 ***Earl of Listowel:*** Minister, you refer in evidence to CEPOL's role in contributing to police training. It was noteworthy in the director of Interpol's contribution last week the great benefit he felt CEPOL had given to his work, training internationally beyond the EU. What specific contribution can it make in the counter-terrorism area?
Ms Blears: We are delighted that CEPOL is now established at Bramshill. It has taken a bit of time for it to get up and running but we are very pleased that it is now starting to produce some excellent work. Its focus is on trying to provide a consistency of training in this field, to try and have benchmarks as standards, to quality assure the kind of police training that happens in Member States around these issues. For example, how to train senior investigating officers, how to train in terms of protective security, making sure all those courses are consistently of a very high standard indeed. It is not a volume training provider in itself. It is much more about accrediting and kite marking the training that happens on the ground and about having a network of police training right across the European Union. It brings added value. It is not trying to substitute its activities for what already happens. It is trying to raise the game around this very complex area in terms of what skills are necessary to combat the threat.

Q397 ***Earl of Listowel:*** Thank you for that very helpful reply. I recognise that we wish not to duplicate what others are doing already. However, some training providers do emphasise the importance they feel delivering at least some of the training has in terms of sensitising them to what their clients need. I wonder if there has been any consideration given to a degree of involvement, not just bench marking but to some limited extent providing training? On a related point, could you also describe what means there are of evaluating the work of CEPOL currently?
Ms Blears: It is not a complete division between assuring quality standards and interacting with those colleges providing it. I do not think CEPOL should be a volume training provider because that happens in Member States and I think it would see itself as competition with some of the colleges out there. I think that would be a messy situation for them to be in. Sometimes there is a bridge between preparing for quality standards, for benchmarking and consistency and seeing how that is implemented in terms of what the colleges are able to provide. In this country at the moment we are talking about the possibility of having a policing improvement agency which to some extent will have some of the same kinds of functions in terms of our police service, providing that bridge between sharing good practice and making sure that it gets implemented.

Q398 ***Lord Corbett of Castle Vale:*** Training the trainers?
Ms Blears: Yes, making sure they have the skills to be able to do it but also ensuring that what you have benchmarked and set out as standard is happening and helping to make a difference in all those Member States. These are sensitive issues. You cannot have CEPOL substituting itself for Member States' own training. You make an important point that the division is not entirely that we have done the benchmarking and now it is entirely a matter for you as to what happens out there. That is why it is important to have this networking so that you build in those relationships to try and ensure that your consistent good practice is happening on the ground. It is early days as yet and I think CEPOL's main focus has to be about developing its quality standards and benchmarking before it gets into the implementation

field. In terms of evaluation, again it is very early days. At the moment, the people who attend and who are part of it do a self-evaluation and a self-assessment, but I think CEPOL itself recognises that there needs to be some more vigorous evaluation of the work it is doing in the future.

Q399 ***Chairman:*** Is there anything you think we have not covered that we should have covered or that we ought to take into account in writing our report?
Ms Blears: I do not think so. I have found this session extremely useful in terms of focusing my mind on where that balance properly lies between what we are doing in the European Union collectively and how we can make a contribution to that from our country. I would like to think that we have the balance right. I have no doubt we will continue this debate. My overriding concern at the end of this session, as it was in the beginning, is to try and make sure we get some practical results out of all this international cooperation that enable us to tackle the terrorist threat that is out there.
Chairman: We are extremely grateful to you for coming to this evidence session and for the written evidence that you and your Department provided. Most of all, thank you very much for the very full and frank way in which you have answered our questions. Can we wish you good luck?

Supplementary memorandum by the Home Office

Set out below are responses to the additional questions that arose in the course of the session:

THE COMMITTEE REMARKED UPON THE RELATIONSHIP BETWEEN INTERPOL AND EUROPOL, SUGGESTING THAT THE FORMER WAS SOMETIMES PERCEIVED TO BE THE "POOR COUSIN"

This relationship has been the cause of much comment, although it is difficult directly to compare the two organisations. Interpol's primary role is to facilitate police cooperation of a conventional and bulk nature (post incident and post arrest requests for information and evidence). It supports about 20,000 UK law enforcement cases a year in this way. Europol's role is more specialised: facilitating law enforcement intelligence cooperation, normally at higher thresholds of case significance and sensitivity (pre rather than post arrest). So it supports far fewer UK cases, about 800 p/a.

However, some significant overlap exists, for example in the provision of analytical support and the maintenance of law enforcement databases. Under Ron Noble (Interpol Secretary-General), and certainly post 9/11, Interpol has moved increasingly into the "intelligence" domain of law enforcement work, whilst maintaining its core services. This has increased the overlap with Europol and, naturally, led to comparisons between the two organisations.

As such, there is some truth to the charge of Interpol being a "poor cousin". Europol commands far more Ministerial interest in most EU Member States and within EU structures. The fact that it is an EU body, administered and financed as such, is one obvious reason for this disparity. Indeed, it is a UK Government priority to exercise influence in the EU so that its institutions develop according to UK interests, making Europol's work of particular importance. Europol has also offered support to UK law enforcement in organised crime and terrorism more directly than Interpol.

Relationships between the two organisations have sometimes been poor and characterised by an atmosphere of competition. However, they have improved of late and we would expect the new Europol Director to reach out to Ron Noble to improve matters. Meanwhile, one positive step has been the introduction of a Europol Liaison Officer at Interpol to facilitate information exchange and closer cooperation. The UK was influential in bringing this about and, indeed, the individual filling that role is a serving UK police officer from the Metropolitan Police Service.

THE COMMITTEE ASKED WHY THE UK DOES NOT ASK FOR PASSPORT NUMBERS ON LANDING CARDS

It was Mr Noble himself who registered surprise that he was not required to *record* his passport number on the UK landing card. However, while the immigration service does not *record* the passport number of every third country national, although it can and does do so in certain individual cases, it should be pointed out that every passport is required to be "swept" and the number *automatically checked* against a hitlist of any lost or stolen passports. Moreover, the UK Immigration Service realises the threat that fraudulent documents present to border security, and immigration staff operating the UK's immigration control are trained in forgery detection techniques, in addition to the routine checking against databases at their disposal. It is also worth noting that once "e-borders" is fully implemented, landing cards will no longer be required, as sweeping machine readable passports will provide the necessary details (those without the coding will be manually

recorded). Furthermore, apart from the UK Checklist, Interpol's (and Europol's) database is a useful and often used resource in trying to establish if a passport is lost or stolen. Once the Schengen Information System II is operational around 2007, all information will automatically be sent to both Interpol and Europol when a Member States uses SIS II (at present each Member State is required to do this).

THE COMMITTEE WISHED TO KNOW THE AMOUNT OF RESOURCES THE UK PROVIDES TO EUROPOL. IN ADDITION, HOW CAN WE ENSURE THIS MONEY IS SPENT WISELY AND COST EFFECTIVELY?

UK subscription to Europol in 2004 was €9.238 million; for 2005 it will be €9.423 million. (Incidentally, this is about four times larger than the UK subscriptions to Interpol).

This is a large investment and it is fair to say that our return on it has not yet been fully realised. It is, therefore, a top priority for the Home Office and NCIS to pursue a Europol policy that maximises efficiency and performance output. We have done this by focusing, inter alia, on introducing intelligence-led principles and outputs at Europol; stronger financial and other governance processes (including on measuring performance); and a high level of scrutiny by Member States of budget proposals and proposed objectives. In these areas we have succeeded largely in delivering real influence. But our work is not done and we look to the UK Presidency and our chairmanship of the Europol Management Board as opportunities for further progress.

THE COMMITTEE ASKED FOR THE VIEWS OF OTHER MEMBER STATES ON EU INTELLIGENCE ISSUES

There is clearly consensus for the measures relating to information exchange, as set out in the EU Action Plan on Combating Terrorism and in the Hague Programme. All Member States agree that information sharing is at the heart of law enforcement co-operation against serious and organised international crime, including terrorism. Improving the flow of information between law enforcement authorities, while respecting key data protection principles, is therefore a priority across the EU.

In addition, Member States are agreed on the need for policy discussions in the Council on matters related to counter-terrorism to be properly informed by comprehensive analytical threat assessments. This has led to the creation of the CT Cell with the EU Joint Situation Centre, which will draw on assessed intelligence from Member States in producing EU-wide threat assessments. There is also broad agreement on the limits to formal EU co-operation on intelligence issues. Member States recognise that the informal operational co-operation that exists between their security and intelligence services is strong. As such, there is no consensus for the development of any new EU structures in the area of intelligence gathering.

I hope that these answers provide clarification, but will be happy to provide any further information that you may require.

Hazel Blears, MP
22 December 2004

Written Evidence

Memorandum by Eurojust

Justification

Does the fight against terrorism require greater operational co-operation and freer exchange of data between law enforcement agencies (both national and EU)?

It is difficult to envisage giving a negative answer to either part of this question.

Nationally the arrangements for co-operation are better in some EU jurisdictions that in others. The extent of operational co-operation is often dependant upon the way the intelligence, investigative and prosecution agencies are organised in each EU state. Where there is national overview or a co-ordinator, as there is in the UK, co-operation is better than where the responsibility for the investigation and prosecution of terrorism may be regionally based or where there are no formal mechanisms for national co-ordination.

Data Exchange

The Commission calls for the establishment of the principle of equivalent access to data by national law enforcement agencies in the EU. To what extent would this challenge the fundamental legal and constitutional principles of member states?

Eurojust is comprised of national members who are investigators and prosecutors with experience in the criminal law of the individual Member States. We do not feel that we have sufficient competence or expertise in the constitutional laws of the Member States to answer this question.

The Commission calls for the interoperability of EU databases. What are the implications of a facility for transferring data between databases of member states? Is there a case for a centralised database for all law enforcement purposes?

We do not feel we have sufficient knowledge or experience to reply to this question in relation to intelligence databases.

The quality of any database and any information drawn from it will always be directly proportional to the amount and quality of the information which is put into it. The creation of a joint intelligence, police and judicial database would have advantages but would be unacceptable to many Member States.

Judicial databases vary and differ in extent widely across the Member States. One of the key factors will be the capacity for all Member States to contribute to any judicial database which is to be created. A key requirement will be the ability of each member state with a database to contribute good quality information, and crucially to transmit such information by secure means. The creation of a secure database to receive, process, analyse and transmit information will be expensive. In a Council Decision made initially on 19 December 2002 the EU Ministers for Justice and Home Affairs decided that Eurojust and Europol should receive a wide range of information about terrorist investigations and prosecutions in the Member States.

Eurojust is developing a capacity within its own ICT infrastructure to build its own database from the EPOC project. This project draws heavily on the information system of the Italian Direzione Nationale Anti-Mafia. Eurojust is unlikely to have the capacity to receive the information suggested by the Council until 2006 at the earliest. Reducing Eurojust's budget in 2004 and possibly in 2005 have and is likely to further delay the installation of such a system.

Of equal importance is the capacity of the judicial authorities in the Member States to transmit and receive information from the database securely. There will need to be common standards of technological infrastructure and secure capacity to transmit the information safely. In many Member States the extent and

use of information technology by competent judicial authorities is at a low level. Consequently many Member States are likely to find putting in place such facilities a considerable financial burden. Until such secure systems are in place, the effectiveness of any judicial or police database developed by Eurojust or indeed any other EU body, is likely to have to operate at a reduced capacity.

Additionally in this general area the Commission is considering making a proposal to allow better access to Registers of Criminal Convictions held in EU member states. Eurojust is to consider offering itself as a location to host this important work. Such consideration is at a very early stage and will of course be subject to wider approval and to the availability of sufficient resources to make locating the project at Eurojust viable.

The effectiveness and interoperability of databases will also depend on parallel thresholds for the exchange of information and material etc. This means ensuring that inconsistent levels of data protection do not strangle the capacity to share information and so frustrate the very purpose for which the database is being created. The following questions also touch on this point.

Data Protection

Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and transfer of data were increased on the scale envisaged? Is there need for a common EU data protection framework for the Third Pillar, as advocated by the Commission?

There will always be a balance that must be struck. On one hand between the need to fight effectively and trans-nationally against terrorism and on the other the protection of the rights of the individual. The public will expect that personal data used will be accurate and that it will not be stored and made available unnecessarily.

The intelligence and law enforcement agencies must be given the capacity to hold sufficient quantities of data to allow them the best possible opportunity to detect, to intervene and to disrupt planned terrorist activity. Additionally after any terrorist attack any such databases should ensure that all available information can be accessed and used to ensure that the perpetrators are caught and brought to justice. Whilst at the same time members of our communities and society itself expects that personal data held on individuals by governments national and international agencies is accurate used properly and kept only so long as is necessary. The measure of necessity will define the level at which the thresholds for retention etc. Surely the thresholds should be set at different levels for the storage and use of personal data for say terrorism when compared with say minor crime.

There is need for a common EU data protection framework for the Third Pillar. Of more importance, however, than the standard itself is the significance of ensuring that it is agreed at the right level so it is of practical use to all relevant law enforcement agencies, both national and EU. As mentioned in the previous question it is vital that any data protection framework does not strangle the capacity of law enforcement agencies to share information and so frustrate the very purpose for which any databases are being created.

Should there be common standards for the transfer of personal data from EU bodies and the Member States to third countries/bodies, including Interpol?

Yes. The important issue is to agree international and inter-institutional standards at the right level to allow practical application and use of the information to be effective. But agreeing these standards will not be easy. Too many states seem to adopt a very restrictive approach on Data Protection and on personal data issues and to be reluctant to accept the fact that serious crime or even terrorism should be treated as a special case.

The Role of the EU

Is there a need for an EU intelligence policy as advocated by the Commission? To what extent can EU objectives be identified separate from those of the Member States?

Eurojust does not deal in intelligence nor as an organisation do we feel qualified to comment meaningfully on this question.

How important is it to speak with one voice in the international arena in matters involving counter-terrorism co-operation?

Investigation and prosecution of crime remains the responsibility of the domestic investigation, police and prosecuting agencies. A consistent approach from the EU and the bodies which support their activities is highly desirable. It is especially important to develop a consistent voice when supporting their activities and ensuring the sharing of information, and on joint co-operation and co-ordinated action. Eurojust and Europol are trying to ensure that we complement each others work and that we do not send inconsistent or mixed messages to our partners in the national and international law enforcement agencies.

The United Kingdom recently hosted a summit of five Member States ("G5") to examine measures to combat terrorism. Do moves of this kind prejudice EU wide initiatives?

Eurojust was not invited to attend this meeting so detailed comment on any prejudice to EU-wide initiatives is not possible. Eurojust held a strategic meeting in June which was attended by senior anti-terrorist specialists from law enforcement agencies representing the EU member states. From this meeting and from cases handled by Eurojust it is clear that a number of member states appear to have experienced little terrorist activity in their jurisdictions. Some countries: Spain, Italy, Germany, France, Belgium and the United Kingdom are involved more regularly in anti-terrorist activity. We can see clear advantages in the competent authorities in these countries meeting together more regularly at an operational level to discuss issues of mutual concern and joint actions. Eurojust is happy to continue to facilitate such co-operation and co-ordinated activities. Meetings such as the G5 summit can enhance wider EU initiatives and focus on the immediate problems of the states where a consistency of approach, immediate action and strategic actions will have immediate effect and which can benefit those with less involvement in the longer term. Without sight of the agenda or outcomes of such meetings it is difficult to judge whether they will prejudice EU-wide initiatives. Some transparency towards other member states and engagement with the Commission and others would also probably help to avoid prejudice.

Institutional Arrangements

What is the added value of the post of EU Counter-terrorism co-ordinator? What should his role be?

We feel the title of the post of "EU Counter-terrorism co-ordinator" is misleading as it suggests that this is an operational role which clearly it is not. The value added by this post is, we think, to build a bridge between the national operational authorities dealing with terrorism and the EU bodies involved in the fight against terrorism such as Eurojust and Europol on the one hand and, ultimately, politicians on the other. The role should help to identify where there are operational and legislative weakness and ensuring that they are addressed at a political or legislative level by the Council. The post holder also has an ambassadorial role on behalf of the EU to external allies both in Europe and for example with the USA. To some extent this role is one which could be said to overlap with the work of Eurojust and Europol. But in practice there are advantages in having a single individual focussed on one topic, terrorism, who is able to speak with consistency and to a range of different parties at a strategic level. There are particular benefits and advantages in being able to bring pressure to bear through his direct reporting line into the EU Council and its Secretariat. This leaves Eurojust and Europol to focus on and improve casework co-operation and co-ordination in terrorist matters and in other case types within their broader brief at a practical and operational level.

What changes are called for in the EU's arrangements (including Eurojust, Europol, the Chief Police Officers' Task Force and the Terrorism Working Group) in order to combat terrorism more effectively?

It is unlikely that the EU would have created Eurojust, Europol, the EU Police Chiefs' Task Force and the Terrorism Working Group in their current format had there been a specific need to respond to terrorism from nothing. There is a need to build structures to ensure the inter-operability and harness the potential and maximise the effectiveness of the EU's JHA arrangements.

Eurojust currently runs regular meetings on terrorism for investigators and practitioners. The latest meeting was in June and was very well received. We are gaining more expertise. It was successful, and so much so that the USA authorities heard and have asked for a similar meeting to be arranged with leading EU countries so they can send senior representatives to attend and share experiences. This is likely to take place later this year.

The domestic competent authorities are responsible for the detection and prosecution of crime. The work of Eurojust, Europol and the PCTF should be examined more closely to ensure there is no duplication of effort and that we all represent value for money and provide the correct level of operationally effective support to the domestic competent authorities.

To some extent the organisations are too polarised. They were created separately to serve police and judicial service in criminal justice systems which are not only different but which have different responsibilities within those systems. For example a police superintendent in England and Wales may have more in common with a "*juge d'instruction*" in France than with a *capitaine* in the French Gendarmerie who might be seen initially as his/her natural equivalent. The 27 or more legal systems which these EU organisations are serving are very different and so it is perhaps no surprise there are some overlaps. But it is in the crucial area of improving action against organised crime and especially in counter-terrorist action that they must work better together. Police and investigating judges/prosecutors are naturally divided for legal, cultural and historical reasons in many EU states. But in fact there are many links between the police and judicial authorities. Even in those states where the responsibilities are quite separate, many legal systems are developing to bring the work of the police and judiciary more closely together. It is vital to ensure an effective response to terrorism and we think there is merit in an evaluation of the capacity of EU bodies to support the domestic authorities in such cases.

Representatives from Eurojust meet regularly with Europol counterparts on a range of matters including terrorism. Europol's terrorism experts have always been invited and have attended Eurojust's meetings on terrorist matters. Similarly Eurojust has attended the six monthly meetings of the EU Police Chiefs Task Force and Eurojust's representatives have attended and played a full part in the meetings of the sub-group on terrorism established by the PCTF. This type of co-operation is vital and must continue to ensure the relative strengths and capacities of the different organisations and competent authorities are harnessed to the best effect at both the national and EU level.

Advantage and benefits might be gained by the setting of joint objectives and increasing accountability of the EU organisations. But Eurojust, Europol and PCTF rely to a large extent on the national domestic competent authorities to co-operate with them for their capacity to deliver results. So long as the competence for law enforcement remains at national level the effectiveness of the EU law enforcement agencies will only be as effective as the extent of support and co-operation they receive from the member states. This is the practical result of the delicate balance of compromise that was at the heart of the establishment many of the EU's Third Pillar organisations. In theory they should work well if given the support by national authorities that should be apparent from the political agreement of the decisions by which they were created. But if there is an absence of sufficient support in practice then the mechanisms for making them work are less clear.

What contribution can EU level training and in particular the EU Police College (CEPOL) make?

We mentioned above the depth of experience in a number of member states where, unfortunately, there has been a history of terrorist activity. This experience has been gained at great cost both in terms of lives and of resources. Systems must be in place to share both the investigative and prosecutorial expertise which exists with those EU states that have not been involved in such work. Unfortunately the spectre of terrorism is one which all states should be prepared to face and the passing on of expertise is vital to equip the less experienced with the benefits of lessons learned elsewhere. CEPOL is one obvious conduit for sharing such expertise.

Michael G Kennedy
President of the College and
National Member for the United Kingdom

2 November 2004

Memorandum by Europol

Through the Liaison Bureau of the United Kingdom, Europol has received on 10 November 2004 the request to provide evidence (either in writing or oral) before the House of Lords Select Committee on the European Union, Sub-Committee F (Home Affairs).

I would like to express my gratitude for giving Europol the opportunity to submit its ideas to the House of Lords' inquiry into EU Counter—Terrorism activities. Based on the questions given in the call for evidence on this matter, Europol would like to summarise its position as outlined below. Please be informed that this statement is founded on the perspective of Europol's area of activities as the central EU law enforcement authority solely.

Further to the EU Action Plan on Combating Terrorism (Council Secretariat documentation reference No 10586/04 LIMITE JAI 237, 14330/1/04 REV 1 LIMITE JAI 428) and the future political orientations as comprised in the "The Hague Programme" concluded by the European Council held on 4–5 November 2004 (Council Secretariat documentation reference No 14292/04 CONCL 3), Europol is of the opinion that the initiative of the Commission for an "EU Information/Intelligence Policy" (Council Secretariat documentation reference No 10745/04 ENFOPOL 77 + COR 1) is of crucial importance to the future effective interaction between the relevant authorities on EU as well as on national level.

The Europol Convention requires that Europol's position with regard to corporate governance issues, such as EU Counter Terrorism activities, is defined by the Europol Management Board as the competent policy decision-making body of EU Member States. In compliance with this principle, all relevant communication to the Article 36 Committee for information of and/or decision by the EU Council is carried out by the Europol Management Board.

At the Europol Management Board Meeting held on 15–16 September 2004, Europol's considerations on the Commission initiative for an "EU Information/Intelligence Policy" were taken note of. The Europol Management Board Presidency Chairman agreed on 3 November 2004 that Europol could follow the strategic suggestions as comprised in the enclosed document (Europol documentation reference No 2651-10r1—#90330v5). The Commission, Directorate General Justice and Home Affairs and the Council Secretariat received this position paper on 1 December 2004 as well.

From Europol's perspective, the key to effective counter terrorism activities lies within the management of information and intelligence on national as well as EU level. Europol therefore shares the Commission's view on the interoperability of EU databases.

It has however to be emphasised that it will be essential to interlink the right information available within the EU. Whether this should (even) be achieved by central data storage or by interlinking several systems, is a matter of holistic business planning and subsequent implementation. From Europol's point of view, new information systems should only be created after it has been proven that the business need for such a system can not be realised through existing systems/databases. To achieve both the interoperability between existing systems (on EU level) and to obtain validated information for the requirements to create new information systems, it would be desirable to establish a central EU point of contact for this task. This point of contact could also guarantee that data models of different systems follow a coherent approach, eg in relation to biometric data standards etc. This would finally also include the co-ordination of relationships with the private sector in contractual and procurement matters.

In this context, I would like to outline that the legal and technical framework to interlink information already exists in various ways. To name an example, the Europol Convention provides for a secure channel, both in terms of legal and of operational security, to exchange information between all Member States of the European Union.

Regarding the more general issue of data protection in the third pillar, Europol is of the opinion that there is no need for a new common legal framework as there is already one in place in the field of law enforcement data processing. According to the assessment of Europol, existing legal instruments (Council of Europe Convention 108/1981, Recommendation No R (87) 15, Schengen Convention 1990) ensure data protection standards sufficiently. Also, both the Europol Convention and the Eurojust Council Decision foresee a data protection level for the European key actors in this area that is certainly strong enough, even in comparison with applicable First Pillar legislation. A focus on one single data protection instrument in the third pillar might distract from more urgent questions regarding the use of data for new purposes in existing legislative instruments.

The EU Counter Terrorism Co-ordinator, who was installed by the European Council of 25 March of this year, has introduced important initiatives in the area of implementing counter—terrorism legislation in the Member States, and is insofar supported by Europol (update of the EU Action Plan on Combating Terrorism, Council Secretariat documentation reference No 14330/1/04 REV 1 LIMITE JAI 428).

To conclude my statement, I would like to stress that the objective of the different initiatives to improve operational co-operation and effective exchange of data between law enforcement authorities—both on national and EU level—is welcomed and supported by Europol. EU Member States' authorities still appear to be in the process of fully exploiting the possibilities of EU—wide co-operation. Also with regard to the relationship between law enforcement and (security) intelligence services, operational cooperation shows room for improvement (see also status report on the Counter Terrorism Task Force—CTTF at Europol—Council Secretariat documentation reference No 14846/04 LIMITE EUROPOL 56 ENFOPOL 172).

I hope that the above has provided you with an overview on Europol's position towards the current initiatives, especially the intention to establish an "EU Information/Intelligence Policy". Europol will do its utmost to provide specific services for the competent authorities in the Member States in order to support them in the fight against terrorism.

Kevin O'Connell
Deputy Director of Europol

Memorandum by the Europol, Eurojust, Schengen and Customs Joint Supervisory Authorities

I. Introduction

Sub-Committee F of the House of Lords Select Committee on the European Union is undertaking an inquiry into EU counter-terrorism activities. This opinion has been drafted in response to the Committee's invitation to submit evidence and, specifically, it seeks to answer the following questions, which the Select Committee addressed to the third-pillar joint supervisory authorities:

— Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the Third Pillar, as advocated by the Commission?

— Should there be common standards for the transfer of personal data from the EU bodies and the Member States to third countries/bodies, including Interpol?

II. Data Protection under the Third Pillar

1. The joint supervisory authorities are those bodies established by the Europol Convention, the Council Decision setting up Eurojust, the Convention implementing the Schengen Agreement and the Convention on the use of Information Technology for Customs Purposes. This opinion should therefore be regarded as the evidence of these four joint supervisory authorities.

2. In addition to the right to respect for private and family life guaranteed by Article 8 of the ECHR and reaffirmed by Article 7 of the Charter of Fundamental Rights of the European Union, the new fundamental right to data protection is enshrined in Article 8 of the Charter. The draft Treaty Establishing a Constitution for Europe that includes the Charter, also guarantees in Article I-51 the right to data protection and states that compliance with data protection rules shall be subject to the control of an independent authority.

3. The ECHR allows interference with the right to privacy if necessary for the interests referred to in the second paragraph of Article 8 and when justified by those interests; such interference must take account of the principle of proportionality. Article 8 of the Charter of Fundamental Rights expands on this, stipulating that personal data must be processed fairly for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This legitimate basis has also to fulfil the conditions of proportionality.

4. The 1981 Council of Europe Convention for the Protection of Individuals to Automatic Processing of Personal Data (Convention 108) provides more specific principles for data protection also applicable in the Third Pillar. There is also a Recommendation with specific data protection provisions for the use of personal data in the police sector, which was adopted in 1987 by the Committee of Ministers to Member States regulating the use of personal data in the police sector.[1]

III. EU Counter-terrorism Activities

5. The establishment of an area of freedom, security and justice was a new objective set for the European Union by the Treaty of Amsterdam. The Tampere European Council in October 1999 placed this objective as a priority for the Union and set an ambitious agenda. In its assessment of the Tampere programme, the Commission recently reiterated the need to give the fight against terrorism priority status.[2] Although the Tampere programme already included activities to create an area of security, the terrorist atrocities of September 2001 resulted in a period of extensive activities in the field of counter-terrorism activities. The Madrid bombings of March 2004 further accelerated this process.

[1] Recommendation No R (87) 15, of 17 September 1987.
[2] Communication from the Commission, Com (2004) 401, 2 June 2004.

6. Various Council declarations and many initiatives followed. A horizontal assessment of these initiatives reveals three general developments in combating terrorism: closer co-operation, more processing of personal data (particularly the exchange of such data), and attempts to highlight the links between combating terrorism and tackling other forms of serious crime. Apart from these EU initiatives, many Member States are in the process of extending the competencies of law enforcement agencies and intelligence services.

IV. Data Protection and Combating Terrorism

7. The EU-wide processing of large quantities of personal data, with access for intelligence and law enforcement agencies, is a significant development in the fight against terrorism and serious crime.

8. Recent proposals anticipate the processing of personal data from different sources on an unprecedented scale. The proposal to require the retention of communications data, and the recent agreement with the US concerning personal information on airline passengers are both examples of a new trend involving the collection of information on individuals (and not only suspects) with a view to aiding the prevention, investigation, detection and prosecution of crimes and terrorism.

9. There is a requirement to assess these developments in the light of the principles of data protection. However, the existing joint supervisory authorities (Europol, Eurojust, Schengen and Customs) have a specific mandate, and there is no existing framework or forum in the Third Pillar with the task of advising and assessing initiatives involving the use of personal data. The Conference of European Data Protection Authorities recently issued a resolution calling on the EU institutions to create an appropriate forum in the Third Pillar to allow for scrutiny of new initiatives involving the use of personal data.

10. Apart from an assessment of the necessity of the proposals referred to in paragraph 8, there is the question whether the current data protection arrangements continue to provide an adequate level of protection for the individual. This question covers two different aspects of data protection.

11. The first is the impact the different proposals may have on individuals. The fight against terrorism and other serious forms of crime is not an isolated activity of one or two law enforcement agencies; it involves a huge number of agencies throughout the European Union. Personal data are processed and analysed with the latest technology and made available to other authorities whenever considered necessary.

The experience of the Europol Joint Supervisory Body in assessing the agreement between Europol and the United States of America demonstrates that limiting the number of law enforcement authorities allowed to process the exchanged data is difficult. In the United States some 1,500 authorities on Federal, State and community level are involved in dealing with criminal offences including terrorism.

12. The processing of personal data on the scale proposed (often involving the processing of information on those who are not suspected of any crime) requires adequate legal safeguards such as purpose restriction, with supervision to ensure that there is compliance with legal instruments.

13. Convention 108 is perhaps too general in its nature to provide for an adequate set of data protection provisions dealing with the new dimension in processing personal data as set out in the different EU initiatives. Furthermore, there are significant differences in the way this Convention has been implemented by Member States in national law.

14. A more specific set of data protection rules for police and intelligence authorities should be developed to enhance the level of data protection. The European Parliament already urged for a binding set of rules. In the recent past initiatives within the Council of the European Union and with the participation of the national Data Protection Authorities to set up a harmonized legal framework failed.

A new legal framework for the Third Pillar, as advocated by the Commission, could provide for this but only if that legal framework provides for a tailor-made set of rules applicable to law enforcement activities. Simply reaffirming general principles of data protection shall not be sufficient. This legal framework could perhaps further elaborate on the principles set out in the Recommendation of the Committee of Ministers to Member States regulating the use of personal data in the police sector including the results of the three evaluations of that recommendation. Any moves in this direction would, of course, have to take account of the existing legislation (particularly the different national approaches to dealing with data protection in the area of law enforcement), the fundamental right of data protection guaranteed in Article I-51 of the Draft Treaty establishing a Constitution for Europe and the increasing convergence of the First and Third Pillars.

15. The second aspect concerns the supervision of the processing of personal data under the Third Pillar. At present the existing national data protection authorities have different competences in the field of law enforcement. This supervision by independent authorities in the Member States should be organised in a way to ensure that these authorities have a common legal basis as referred to in paragraph 14, equivalent powers, and sufficient funds and capacity.

V. Transfer of Personal Data to Third States and Bodies

16. The Europol Convention contains specific rules governing the exchange of personal data to third states or bodies. The basic requirement is that the receiving state or body should have an adequate level of data protection, and that once this has been confirmed a formal agreement should be drawn up. The Protocol to Convention 108 also introduces the adequacy rule but allows derogation if domestic law provides for it because of specific interests of the data subject or legitimate prevailing interests, especially important public interests.[3] Most of the EU Member States have not ratified this Protocol yet.

17. At present there is no uniform Third Pillar instrument regulating the transfer of personal data to third states or bodies. In practice this leads to a situation where Europol cannot transfer data to a particular third state if that state is deemed not to have an adequate level of data protection, but where there is nothing to prevent an EU Member State from doing so by means of a bilateral agreement—there is a need to address this discrepancy.

Peter Michael
Data Protection Secretary

4 October 2004

Memorandum by the National Criminal Intelligence Service (NCIS)

1. The National Criminal Intelligence Service (NCIS) does not have a direct remit for counter-terrorism activities. The distinction, in European matters, is moot. The range of intelligence is a continuum running from simple crime to the most sensitive counter-terrorism intelligence. There are many overlaps and a lot of the techniques are essentially the same. This submission will mainly come from the crime end of the continuum.

2. NCIS produces intelligence on serious and organised crime, including that which funds terrorism, it is also home to the UK national bureau of Europol and I sit on the Europol Management Board. NCIS also runs the UK's network of liaison officers in Europe (including Europol) and hosts the national Interpol bureau. We expect these functions to be consolidated together with a network of overseas liaison officers throughout the rest of the world when NCIS is absorbed into SOCA in 2006.

3. NCIS is (and SOCA will be) a key network for operational co-operation with other EU Member States (MS) and for the exchange of information worldwide. When SOCA is set up it may be necessary to clarify what role if any it will play in the UK's counter-terrorism activities.

4. Justification

5. The target for terrorists has broadened and the fight against them will need greater co-operation and intelligence sharing to ensure the necessary intelligence led response. Any benefit from effective intelligence sharing cannot be justified if it jeopardises the secret and sensitive intelligence sources, which we currently rely on. Greater overt co-operation will act as a deterrent. It needs to be mirrored by parallel covert co-operation between trusted intelligence partners.

6. Events of the last few years (including 9/11 and Madrid) provide all the evidence that is needed on this point. In particular what they demonstrate is the weakness of systems dependent on agencies identifying a specific reason for intelligence exchange. Two agencies will often have no particular prompt for realising they are holding two different parts of the same picture.

[3] Additional Protocol regarding supervisory bodies and transborder data flows, Strasbourg 8 November 2001, Opinion of the Europol, Eurojust, Schengen and Customs Joint Supervisory Authorities.

7. Data Exchange

8. From an operational police perspective the biggest challenge to this concept is the different way in which different legislations treat intelligence material, especially the degree to which it is disclosed in the trial process. There is also a great divergence in the way different MS understand the concept of intelligence, and intelligence led operations.

9. Both ECHR Article 8 and the Data Protection Act have been interpreted as requiring case-by-case consideration of the proportionality of any disclosure of personal data. Such an interpretation presents a challenge to bulk or routine sharing of intelligence.

10. A centralised EU database could be a very powerful tool if it was to concentrate on serious and organised crime; it would enhance the benefits of the intelligence led approach, which we are currently asking Europol to adopt. A database extended to all law enforcement purposes would be unwieldy and would replicate the role of the Sirene bureau and Interpol.

11. Data Protection

12. As suggested above there is an argument that current data protection arrangements inhibit the "speculative" exchange of intelligence (in order to identify whether, for example, common targets exist) since they require the necessity and proportionality of exchange to be identified in advance. Once it is recognised, however, that this sort of speculative exchange has a valuable role in the prevention of terrorism, the balance of the human rights argument should swing decisively in its favour. There may be potential in the use of universally adopted PIN codes for suspects or targets (derivable from an individual's date of birth and name) to limit the privacy intrusion—a match of which (between agency databases) would act as a prompt for further exchange.

13. A common EU data protection legal framework would promote confidence and consistency around intelligence exchange. It would, however, have to be sufficiently broad to take account of different national legislative requirements concerning, for example, the disclosure of unused material in criminal trials.

14. The national security exemptions under section 28 of the Data Protection Act could make the exchange of data easier on these grounds, but as there is currently no common definition of national security across the EU it is probably not safe to rely on this.

15. Common standards for transfer to third countries/bodies would similarly help to promote confidence and consistency; but would also have to take account of differences between legal systems.

16. The Role of the EU

17. An EU intelligence policy would need to start with an agreed definition of the concept of intelligence. A common European intelligence policy based on an intelligence model (as we have in the UK with the National Intelligence Model (NIM)) would allow EU ministers to reflect EU priorities in the focusing of intelligence gathering priorities. Operational activity would follow led by the intelligence. This process could focus law enforcement effort on organised crime which funds terrorism.

18. We are not sure that the same model necessarily applies to intelligence agency material. Intelligence agencies have traditionally adopted an intelligence led approach and the importance of sensitive intelligence, as outlined above, means it needs special handling. We are not the experts in the area of secret counter-terrorism intelligence. Incorporating intelligence agencies into the same model as law enforcement may concern some MS, especially the Eastern European accession states.

19. The G5 meeting was useful in identifying some common themes to the current terrorist threat within a manageable forum. As such it acted as a catalyst for the exchange of ideas between long standing partners who are arguably the prime terrorist targets in Europe. We think that this should inform rather than prejudice EU wide initiatives.

20. Institutional Arrangements

21. We think that the role of the EU Counter-terrorism Co-ordinator should be as a coordinator of EU wide interests rather than either policy maker or spokesman. There is a need for someone to act as a broker matching requirements with expertise and capability. This need extends to post incident management and forensic recovery.

22. In the event of an incident the authorities involved do not necessarily want an unfocussed influx of experts. The co-ordinator could act as a one stop shop able to organise an effective and appropriate response.

23. We think that all the EU bodies mentioned need to be rationalised as far as possible through a coherent intelligence led framework embedded in the structures of the EU. We think the organising committee envisaged in the draft Constitutional Treaty would be an appropriate structure to give this kind of focus.

24. EU level training would contribute to the capacity for joint working. It would also reinforce mutually acceptable standards, particularly in evidence gathering where there is the possibility that that evidence will be transferred across jurisdictional boundaries.

Peter Hampson, CBE, QPM
Director General

7 September 2004

Memorandum by the National Crime Squad (NCS)

1. The remit of the National Crime Squad (NCS) is to combat national and international serious and organised crime. It does not have a specific remit for counter-terrorism. However, the NCS may provide support to UK agencies who do possess such a remit. The NCS is aware of the existence of links between terrorism and organised crime. When such intelligence is detected by the NCS, it is disseminated to the relevant agencies. As Head of the UK delegation to the European Police Chiefs Task Force, I am responsible for coordinating the UK's input into the counter-terrorism work of this body, in consultation with the Association of Chief Police Officers, the Home Office and other law enforcement agencies. I am also responsible for facilitating the counter-terrorism work of the G8 Roma-Lyon Group's Law Enforcement Projects Sub-Group in my role as Chair of the Group.

2. In recent months the NCS has responded to Home Office requests for comments on some of the proposals highlighted by the Select Committee for facilitating data exchange within the EU, in particular the draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement agencies. The NCS has an interest in such proposals given that they will have an impact not only on EU counter-terrorism cooperation but also on the broader issue of EU law enforcement cooperation.

Justification

3. The NCS believes that the fight against terrorism does require much greater operational co-operation and freer exchange of data between law enforcement authorities both nationally and internationally. To a greater or lesser extent, partnership working is a reality for all agencies within the UK. The negotiation of partnership agreements would be facilitated if dedicated partnership managers existed within all agency structures.

Data Exchange

4. The NCS believes that there is a case for a centralised EU database for all law enforcement purposes. However the feasibility and ultimate potential of such a database would need to be carefully assessed. Legislative and linguistic obstacles and the conversion of records into new and standardised formats would cause most difficulties. Costs may be prohibitive when compared with the benefits accrued.

Data Protection

5. There should be common standards for the transfer of data from EU bodies to member states or third countries which should protect the individual when data is being transferred. A common EU data protection legal framework should not be ruled out. The Section 28 exemption of the Data Protection Act, 1998 (DPA) may provide a sufficient legal basis for the exchange/collection of personal data. This would provide exemption in relation to National Security issues and personal data from any of the provisions of:

— The eight Data Protection Principles.

— Part 11 (individuals rights), Part 111 (Notification) Part V (Enforcement) Section 55(1) (which prohibits the unlawful obtaining of personal data; a person will not be found guilty of this offence if the personal data in question falls within the National Security exemption).

Statutory Instrument 2000 No 206 re Data Protection Tribunal (National Security Appeals) should be considered when judging if this exemption would be sufficient. If the National Security exemption does not provide sufficient legal basis, consideration must be given to the issue of who is the Data Controller of the

information once it is passed. If member states were not to become Joint Data Controllers, a Data Processing Agreement would be necessary. If a member state is the Data Controller of the information once passed it is essential that safeguards are in place for secondary processing of information once it has been transferred. If Data Controller status stays with the providing State, consideration needs to be given to:

— Who is it being shared with?
— Will there be direct access to the database?
— What medium will be used for the transfer of information?
— What Protective Marking level should be given to the data?
— What is the security status of the infrastructure to be used?
— What security provisions are in place once the information has been passed?

The Role of the EU

6. There is a need for an EU Intelligence Policy in order to promote intelligence-led policing throughout the EU and to improve the ability of EU member states to effectively combat organised crime and terrorism. The framework for such a policy can be based on the UK's National Intelligence Model (NIM). The NCS has supported efforts to promote specific initiatives to develop intelligence-led policing in the EU, for example through the European Police Chiefs Task Force and Europol.

Institutional Arrangements

7. In its Declaration of 25 March 2004, the European Council underlined the role of the European Police Chiefs Task Force (ECPTF) in coordinating operational responses to, and prevention of, terrorist acts and called on the EPCTF to review how its operational capacity could be reinforced. A number of reform initiatives are underway as a result of this request. The NCS has supported proposals to establish, within the EPCTF framework, small operational teams made up of interested EU member states who would take forward intelligence-led joint operations based on an improved Europol intelligence assessment. The NCS has also supported proposals to move the EPCTF to within EU Council structures. This issue is still under discussion but may be agreed upon by the European Council before the end of the year.

8. The NCS believes that bodies such as Europol and the EPCTF should concentrate on adding value to the EU's counter-terrorism activities in areas where law enforcement has a particular role to play. This includes analysing criminal intelligence, sharing and developing best practice in policing at a community level in the prevention of terrorism, or sharing best practice to ensure that effective contingency plans, including planning for post-incident investigations, are in place.

William Hughes
Director General

10 September 2004

ISBN 0-10-400628-5

9 780104 006283

Printed in the United Kingdom by The Stationery Office Limited
3/2005 994175 19585