HOUSE OF LORDS

European Union Committee

9th Report of Session 2006–07

Schengen Information System II (SIS II)

Report with Evidence

Ordered to be printed 20 February and published 2 March 2007

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 49

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)
Environment and Agriculture (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 Brown of Eaton-under-Heywood
Baroness Cohen of Pimlico
Lord Freeman
Lord Geddes
Lord Grenfell (Chairman)
Lord Harrison
Lord Kerr of Kinlochard
Lord Maclennan of Rogart
Lord Marlesford
Lord Powell of Bayswater
Lord Roper
Lord Sewel
Baroness Symons of Vernham Dean
Baroness Thomas of Walliswood
Lord Tomlinson
Lord Wright of Richmond

The Members of the Sub-Committee which carried out this inquiry (Sub-Committee F) (Home Affairs) are:

Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Baroness D'Souza
Lord Foulkes of Cumnock
Lord Harrison
Baroness Henig
Lord Jopling
Earl of Listowel
Lord Marlesford
Lord Teverson
Lord Wright of Richmond (Chairman)

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

Note: 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

FOREWORD—What this Report is about

The Schengen Information System (SIS) is an EU-wide system for the collection and exchange of information relating to immigration, policing and criminal law, for the purposes of law enforcement and immigration control. The System raises fundamental questions concerning the balance between, on the one hand, the operational effectiveness of immigration control and public security by law enforcement authorities, and on the other hand the protection of civil liberties. It is against this potential conflict that the Committee has examined the working of the SIS, and its planned development into a second-generation system, known as SIS II. We have looked at SIS II with the aim of assessing whether the proposed system is efficient, transparent, accountable and secure.

The United Kingdom is not one of the full Schengen States, because it maintains its border controls with other Member States. It will therefore be denied access to immigration data on SIS II, although it will have access to other data for the purposes of police and criminal cooperation.

SIS II will store an enormous volume of sensitive personal data. The processing and protection of such data will be governed by many different legislative instruments, often conflicting. We consider how the provisions should be made clear and unambiguous, and whether the United Kingdom should have access to all the data.

We have also looked at the delay in setting up SIS II, and the consequences this will have for the United Kingdom and for other Member States.

Schengen Information System II (SIS II)

CHAPTER 1: INTRODUCTION

The subject of our inquiry

1. One of the main aims of the Treaty establishing the European Economic Community, signed in Rome almost exactly half a century ago, was "the abolition, as between Member States, of obstacles to the free movement of goods, persons, services and capital". Chief among such obstacles was of course the checks imposed at the borders between the States. Even then, progress had been made towards the abolition of some of those obstacles between three of the six original Member States, Belgium, the Netherlands and Luxembourg, by the Benelux Customs Union, which became operative in 1948, and subsequently by the Benelux Economic Union.

2. By 1985 considerable progress had been made towards relaxing border controls on the movement of goods, services and capital, but restrictions on the movement of persons other than workers remained. Five of the (by then) ten Member States[1] were frustrated by the slow progress, and in that year France and Germany joined the Benelux countries in an agreement which was "prompted by the resolve to achieve the abolition of checks at their common borders on the movement of nationals of the Member states of the European Communities and to facilitate the movement of goods and services at those borders".[2] That agreement was signed in the Luxembourg border village of Schengen on 14 June 1985.[3]

3. The principal purposes of border checks on persons include keeping the unwanted out—for example, undesirable aliens—and preventing the wanted from leaving, chiefly those suspected of criminal offences. Those manning the borders need of course to have detailed information about such persons. If border checks between two countries are reduced or eliminated, as a compensatory measure that information needs to be shared at the external frontiers of both countries. Without this pooling of information, a fugitive wanted in France and seeking to escape to England could simply travel to Belgium without any check at the border, and cross from Belgium to England through a border where his name would be unknown to Belgian frontier guards. The 1985 Schengen Agreement, a brief document setting out matters of principle, said nothing about the sharing of information, but the 1990 Convention which fully implemented the Agreement[4] created a multinational database for the use of immigration, border control, judicial

---

1 The United Kingdom, Ireland and Denmark joined the original six Member States (the Benelux, France, Germany and Italy) in 1973, and Greece in 1981. The Treaty of Accession of Spain and Portugal was signed in 1985, but the accession did not take place until 1986.

2 Fourth recital to the Agreement.

3 The 1985 Schengen Agreement is published in OJ 2000 L 239/13.

4 The 1990 Schengen Convention is published in OJ 2000 L 239/19.

and police authorities in any of the States which fully apply the Schengen Convention: the Schengen Information System (the SIS).

4. The Schengen Convention was incorporated by the Treaty of Amsterdam as part of the law of the EU, and now extends fully to all the fifteen States which were members of the EU before the 2004 and 2007 accessions other than the United Kingdom and Ireland, and also separately to Norway and Iceland. But the SIS is no longer adequate for this purpose. It is therefore being replaced by a second generation Schengen Information System. It is this—SIS II—which is the subject of our inquiry.

5. Initially, the main perceived need for a new version of the SIS was to accommodate the inclusion of the EU's new Member States, since the initial design of the SIS had not provided for the participation of more than 18 States. (Q 422) But a second perceived need was to take the opportunity provided by the creation of a new system to allow the inclusion of biometric data.

Reasons for the inquiry

6. The computer database of SIS II is of the same order of magnitude as some of the largest United Kingdom public service databases. As so often with these, problems have arisen in the course of establishing SIS II which have caused considerable delay. We have examined the reasons for this, the consequences of the delay (especially for the newer Member States), and an interim solution which has been adopted to cater for this, and which may itself cause further delay.

7. A database of this size, with immense lists of wanted and unwanted persons and objects, raises major data protection issues. We have looked at the adequacy of the data provisions, and the potential for conflict between them. Inaccuracies in the information stored could lead to the wrong persons being stopped at borders or arrested, or to persons being allowed to pass freely who should have been stopped. We have considered whether the use of biometric information would enhance the accuracy of the system.

8. United Kingdom Governments have never shown any enthusiasm for the reduction and eventual elimination of checks at frontiers. We have retained our border controls, and our right to do so is recognised by the Treaty of Amsterdam.[5] Ireland, since it is part of the common travel area, is in the same position. The special position of the United Kingdom was the subject of our report *Schengen and the United Kingdom's Border Controls,* published in March 1999.[6] That report considered the position of the United Kingdom in relation to the SIS.[7] But in the last eight years much has changed, and the current position of the United Kingdom was considered during this inquiry.

Conduct of the inquiry

9. In June 2006 we issued a call for written evidence which is reproduced in Appendix 2. In reply we received evidence from eight persons and bodies. In the course of October and November 2006 we heard oral evidence from

---

5 Protocol on the position of the United Kingdom and Ireland, annexed to the Treaty on European Union and the Treaty establishing the European Community.

6 7th Report, Session 1998–99, HL Paper 37.

7 Paragraphs 34–40 of the report.

24 witnesses, including six during a visit to Brussels on 27 and 28 November. We are most grateful to all those witnesses who sent us written evidence and gave us oral evidence.

10. Throughout the inquiry we have had as our Specialist Adviser Steve Peers, Professor of Law at the University of Essex Centre for European Law. His unrivalled knowledge of the subject has been of the greatest assistance to us. We are very grateful for all his help.

Structure of this report

11. In the following chapter we look in more detail at the chronological and legislative background, and in chapter 3 at how the system works in practice. Chapter 4 considers how it is and should be managed, and chapter 5 the access to the data. In chapter 6 we look at the data protection issues, while chapter 7 investigates the special position of the United Kingdom in relation to immigration data. Finally we summarise our conclusions and recommendations. **We recommend this report to the House for debate.**

CHAPTER 2: BACKGROUND—THE DEVELOPMENT OF THE SCHENGEN DATABASE

Schengen and SIS

12. The 1990 Schengen Convention provides in Articles 92–119 for the establishment, operation and use of the SIS, and for protection of the data contained in it. Articles 94 to 100 divide the data entered in the SIS into a number of different categories of "alerts". The word "alert" is used in a technical sense, and is defined in relation to SIS II as "a set of data entered in SIS II allowing the competent authorities to identify a person with a view to taking specific action".[8] The categories of alert are:

    (a) persons wanted for extradition to a Schengen State (Article 95);

    (b) a list of non-EU citizens ("third-country nationals") who should in principle be denied entry to any of the Schengen States (Article 96);

    (c) missing persons or persons to be placed under police protection (Article 97);

    (d) persons wanted as witnesses, or for the purposes of prosecution or the enforcement of sentences (Article 98);

    (e) persons or vehicles to be placed under surveillance or subjected to specific checks (Article 99); and

    (f) objects sought for the purpose of seizure or use in criminal proceedings (Article 100).

13. Each Schengen State decides which of its law enforcement and immigration control authorities are to have access to some or all categories of SIS alerts, and for which purposes. If a national authority finds that a particular individual or object is listed in the SIS, this is known as a "hit". The following are examples of the way the system works.

BOX 1

Examples of the Schengen Information System in action

A consulate of one of the Schengen States is considering an application for a short-term visa, which will be valid for visiting all of the Schengen States (this is known as a "Schengen visa"). The consequence of a hit is that in principle the visa application must be refused.[9]

A person in police custody is the subject of an extradition request or a European Arrest Warrant (EAW), which is listed in the SIS. A hit would usually result in the arrest of the fugitive and the subsequent transmission of further documentation relating to the extradition request or the EAW, so that the process of extraditing or surrendering the fugitive can get under way.

A police officer checks the SIS to see whether a vehicle with foreign licence plates is listed as a stolen vehicle in an alert in the SIS. The hit on the stolen vehicle would trigger bilateral contacts between the national authority which made the hit and the national authority which issued the alert.

8 This definition is taken from Article 3(a) of the Regulation on the setting up of SIS II (OJ 2006 L 381/4), but is equally relevant to the original SIS.

9 See Article 15 of the Convention, read in conjunction with Article 5.

14. The current SIS began operations in March 1995, when the Schengen Convention was first fully put into force for an initial group of seven Member States.[10] The Convention was later extended, and by March 2001 it applied fully to all of the first fifteen EU Member States, except the United Kingdom and Ireland.[11] The Convention also applied by that date to the associated States of Norway and Iceland.

15. In the meantime, the legal framework for the Schengen Convention and the measures building on it (known collectively as the "Schengen *acquis*") altered fundamentally on 1 May 1999, when the Treaty of Amsterdam came into force. This Treaty aimed to integrate the Schengen *acquis* into the EU's legal order. This meant that the existing Schengen *acquis* would henceforth be treated as if it were EU law, and that all future measures building on that *acquis* would be adopted according to EU decision-making procedures. These procedures differ according to the different legal bases in the Treaties which confer power upon the EU institutions.

16. Accordingly the Council was obliged to adopt a decision allocating all of the Schengen *acquis* in force as of 1 May 1999 to a legal basis in either the EC Treaty (which among other things deals with economic integration, including immigration law) or the EU Treaty (which deals with the EU's Common Foreign and Security Policy—the "second pillar"—and cooperation in criminal law and policing—the "third pillar"). The Council was able to agree on allocating the entire Schengen *acquis* to a legal base in the "first pillar" (the EC Treaty) or the "third pillar" (the policing and criminal law provisions of the EU Treaty), except for the provisions concerning the Schengen Information System.[12] The reason the Council was unable to agree on the allocation of the SIS provisions was that they applied simultaneously to data concerning immigration (which in principle should be subject to legal bases in the "first pillar" EC Treaty) and to data concerning policing and criminal law (which in principle should be subject to legal bases in the "third pillar" part of the EU Treaty).

17. As a result, by way of default, all SIS provisions are regarded as falling within the third pillar (policing and criminal law). However, the Treaty of Amsterdam requires that any new measures "building upon" the Schengen *acquis* which was in force back in May 1999 have to be adopted using the correct legal bases. So, despite the failure to agree on the "legal base" for the SIS provisions in the Schengen *acquis*, it is necessary to use the relevant EC Treaty "legal bases" for any new measure concerning SIS immigration data to be adopted after May 1999.[13]

The United Kingdom position

18. When the Schengen *acquis* was integrated into the legal framework of the EU by a Protocol to the Amsterdam Treaty,[14] the United Kingdom gained the possibility to request participation in all or part of that *acquis*, subject to

---

10 Belgium, France, Germany, Luxembourg, Netherlands, Portugal and Spain.

11 See paragraphs 18–19.

12 The decision allocating the *acquis* can be found in OJ 1999 L 176/1.

13 Modest amendments to the current SIS were given effect by an EC Regulation and an EU third pillar Decision adopted in 2004 and 2005, which among other things gave access to Europol and Eurojust. (OJ 2004 L 162/29, and 2005 L 68/44).

14 Protocol integrating the Schengen acquis into the framework of the European Union.

approval by the unanimous consent of the Schengen states. To that end, the United Kingdom requested and gained approval in 2000 to participate in all of the Schengen *acquis* provisions concerning criminal law and policing (except for cross-border hot pursuit by police officers).[15] This also entailed participation in the SIS, as regards criminal law and policing information, but not the SIS immigration data, concerning the list of persons to be denied entry into the Schengen States. The Schengen provisions in which the United Kingdom had been given permission to participate were put into effect for this country from 1 January 2005.[16] The United Kingdom should have been ready to be linked to the SIS database by late 2004, but to date it has failed to connect to the system. Home Office officials told us that this proved impossible due to technical difficulties and "acts of God", such as a fire which destroyed some equipment. (Q 8)

19. The later application of Ireland to participate in the same provisions of the Schengen *acquis* as the United Kingdom (except for the provisions on cross-border police surveillance) was approved in 2002,[17] but has not yet been put into effect in any respect.

The need for SIS II

20. As we have said, initially the main purpose of a new version of the SIS was to accommodate the inclusion of the EU's new Member States. The creation of a new system was also seen as an opportunity to provide for additional technical features, in particular for the inclusion of biometric data (data directly concerning the physical characteristics of individuals, such as photographs, fingerprints, DNA profiles or retina scans).

21. In the event, neither the United Kingdom nor Ireland has sought to opt in to the measures concerning SIS II immigration data, but they will both be covered by the measures concerning policing and criminal law data, as well as concerning access by vehicle registration authorities to data on stolen vehicles (see further discussion of the new SIS II legislation in paragraphs below). We consider in chapter 7 whether the Government should attempt to obtain access to some of the SIS II immigration data, and to share United Kingdom immigration data with other Member States.

The timetable of SIS II

22. The initial intention was to implement SIS II in 2007, in parallel with the extension of the Schengen area to the EU's new Member States (the ten Member States joining in May 2004).[18] When, as far back as 2001, the Council entrusted the Commission with the development of SIS II, its mandate ran to 31 December 2006; five years was thought to be generous. But following the Commission's award of the tender for the SIS II project, a disappointed tenderer brought legal proceedings against the Commission.

---

15 OJ 2000 L 131/43.

16 OJ 2004 L 395/70.

17 OJ 2002 L 64/20.

18 See the Hague Programme, adopted on 5 November 2004, paragraph 1.7.1: "The European Council urges the Council, the Commission and Member States to take all necessary measures to allow the abolition of controls at internal borders as soon as possible, provided all requirements to apply the Schengen acquis have been fulfilled and after the Schengen Information System (SIS II) has become operational in 2007."

The Court of First Instance[19] suspended the award of the tender until its interim ruling, in which it strongly criticised the Commission's conduct in issuing the tender, but nevertheless allowed it to proceed. The case was subsequently settled.[20]

23. This was the main cause of delay, but there was no lack of other delaying factors. There was uncertainty regarding the sites for the development until agreement was reached that the main site should be in Strasbourg, with the back-up site in Sankt Johann im Pongau, in Austria. Problems arose with the air-conditioning which is an important feature of such a project. (Q 5) The implementation of the SIS II contract by the successful tenderer ran into difficulties; the Commission admitted that it did not sufficiently supervise the tenderer, due to a lack of qualified staff. (Q 392) And finally, in the Commission's own inimitable words, "the complexity of the project itself also had a negative impact on the planning"[21]—a fact which should come as no surprise to those familiar with the fate of similar projects in this country.

24. In July 2006 the Commission accordingly proposed that its mandate should be extended to 31 December 2007, and this was agreed. But barely two months later the Commission proposed an extension of its mandate by a further year, to 31 December 2008.[22] No further reasons were given for this either by the Commission or by the Home Office in their Explanatory Memorandum on the proposal. Nevertheless, this further extension was also agreed.[23]

25. The A8—the ten Member States which acceded in May 2004, less Cyprus and Malta—believe they are being treated as second class States from the point of view of free movement of persons. They had been led to believe that they would join the Schengen area by October 2007, and this date had been re-affirmed by the European Council in June 2006. They had been anxiously awaiting SIS II coming into operation, and were dismayed by these delays. Some of them had invested considerable resources to ensure that their internal record systems would be of a standard which would enable them to join. We heard an eloquent speech to this effect from the Chairman of the Constitutional Rights Committee of the Estonian Parliament. At a joint meeting in November 2006, the foreign ministers of the Visegrád countries[24] and the three Baltic States were still pressing for adherence to the original timetable.

26. In October 2006 Portugal put forward a proposal, which it called "SIS one4all", to allow the SIS to be adapted to include the A8, so enabling them to join Schengen by October 2007.[25] Some of those States were initially unenthusiastic, believing that they should not accept a halfway house; other States, and not just the A8, feared that this would further delay SIS II. The Commission believed that it would add nine months to the planning of SIS II. Nevertheless on 5 December 2006 the Justice and Home Affairs

---

19 The Court of First Instance is attached to the Court of Justice to hear designated categories of cases. There is a limited right of appeal to the Court of Justice on points of law.

20 Capgemini Nederland BV v Commission, Case No T 447/04, [2005] ECR II-257

21 Explanatory memorandum to the proposal for the extension of the mandate in Document 11746/06.

22 Document 12737/06.

23 OJ 2006 L 411/1 and L 411/78.

24 Czech Republic, Hungary, Poland and Slovakia.

25 Document 13540/06.

Council, after re-affirming that "the development of the SIS II remains the absolute priority", decided to implement SIS one4all for the A8, and invited the Commission to present yet another revised timetable for SIS II by February 2007.

27. Since the requirement to develop a new generation of the SIS was apparent many years ago, in the light of the planned enlargement of the EU, there was an opportunity for long-term strategic planning of the project, which could have avoided the delays and reduced the costs which have affected the SIS II project. This opportunity was missed. There are lessons to be learned by the EU as regards the planning and development of other large-scale multinational information systems.

The United Kingdom's timetable

28. As we have said,[26] the United Kingdom does not participate in the current SIS, nor has it any plans to do so. Home Office witnesses told us that their assessment in October 2005 was that SIS I connection for the United Kingdom would not have been achieved by the time SIS II would have been delivered for the rest of the Member States.[27] Ministers decided that efforts should be concentrated on delivering SIS II to a properly robust programme and timetable. The United Kingdom's "aspiration is to join SIS II in 2009. We think we will be ready … all Member States will be connected when the UK will join in 2009." (QQ 8, 11) But Superintendent Mike Flynn, the Director of the Joint Operational Authority of SIRENE UK,[28] was of the view that, once the central system of SIS II was in operation, "the new Member States, of which the United Kingdom will be one, will have a staggered integration into the system, and we would reasonably expect this to be about 2010". (Q 202)

29. The inevitable further delay entailed by SIS one4all might have been bad news for the law enforcement authorities of this country. As it is, unless there is further disastrous slippage in the timetable for SIS II, it will be operative by the time the United Kingdom can be connected. This does not explain why Ministers are content for the United Kingdom to be the last Member State to be connected to it, or for our law enforcement authorities to be the last to benefit from the scheme.

30. **Ministers should put more resources into the development of the national connection to SIS II. Whenever the central system is ready, the United Kingdom should be ready and able to participate as early and as fully as possible.**

31. It does not appear that the Government have considered that the United Kingdom might join SIS one4all. Since this was designed for those States which had plans to join SIS II in 2007, and since the United Kingdom had in any event no plans to join before 2009 at the earliest, no doubt the Government felt that SIS one4all was not relevant and need not affect its

---

[26] Paragraph 18.

[27] Yet as recently as 28 June 2006 the Commission stated, in its Report on the implementation of the Hague Programme for 2005: "The Council Decision on the implementation of part of the SIS by the United Kingdom will be adopted after finalisation of the necessary technical amendments in that Member State" (COM(2006)333 final, paragraph 33)

[28] For an explanation of SIRENE UK, see paragraphs 54–55.

plans. At least, agreement has been reached that the United Kingdom need not contribute to its cost.[29]

The cost

32. The cost of developing SIS II is a charge on the budget of the EU. Since the Commission was charged with the task of developing SIS II at the end of 2001, a total of over €26 million has been committed to this project from the EU budget.[30] According to the Commission's proposed SIS II legislation, the EU budget will be charged a further €114 million between 2007 and 2012 to get SIS II up and running.[31] Of this the United Kingdom pays 18%: a full contribution, despite not having access to all the information on SIS II. (QQ 28–32)

33. The current Home Office estimate for the cost to the United Kingdom of implementing SIS II is £39 million. Additionally there is an annual cost of £500,000 to the Commission for its costs in running the system, and operational costs for running the system in the United Kingdom, the supporting technology and the people to manage it of the order of £3 to £4 million. (QQ 22–27)

Lack of transparency

34. The Commission did not conduct an impact assessment of the SIS II proposals, even though these have become standard for any significant EU legislative proposal. Furthermore, the Commission's legislative proposals for SIS II were accompanied by an explanatory memorandum that only briefly set out the background to the proposals, whereas the explanatory memoranda for proposed EC or EU legislation usually explain the proposed legislative text in detail.

35. In its written evidence, the Commission told us that "the underlying rationale and nature of the system [SIS II] will remain the same as the current SIS. An impact assessment and public consultation were, therefore, not necessary." For the Home Office, Jonathan Sweet repeated this, and did not suggest that there was anything inadequate about this procedure. (Q 33) However in oral evidence Jonathan Faull, the Director-General for Justice, Freedom and Security at the Commission, reassured us that an impact assessment would be carried out before new functions of considerable importance were implemented, such as the full use of biometric data and its use for searches. (Q 387)

36. The Commission had formally consulted several persons and bodies, among them Mr Peter Hustinx, the European Data Protection Supervisor (EDPS). However it seems to us that the Commission did not take his views seriously. In his formal Opinion on the proposals for the legislation, delivered in reply to the Commission's request, Mr Hustinx stated: "It is in many respects difficult to know what the intention behind the texts is; the absence of an

---

29 The initial proposal was uncosted, and we have not seen any estimate of what the costs may be either of SIS one4all itself, or of the consequent delays in SIS II.

30 The exact figure is €26,400,775. This is derived from the EU's annual budgets, which indicated a charge of €950,000 in 2002 (OJ 2002 L 29, p 1054), €500,000 in 2003 (OJ 2003 L 54, p 871), €8,100,775 in 2004 (OJ 2004 L 53, p 1000), €15,800,000 in 2005 (OJ 2005 L 60, p 1078), and €1,050,000 in 2006 (OJ 2006 L 78, p 994).

31 See COM(2005)236, 31 May 2005, page 46.

explanatory memorandum is highly regrettable … Moreover, one can only regret there has been no impact assessment study. The fact that the first version of the system is already in place does not justify this, since there are considerable differences between both."[32]

37. Other witnesses have also regretted the lack of explanatory material. We share this view. In the light of the considerable cost and resource implications for all Member States (including the United Kingdom) resulting from the development of SIS II, an impact assessment was obviously desirable. The existence of the prior agreement of the Council on SIS II is no answer. As for the explanatory memorandum, the extensive changes which the Commission proposed to the current SIS merited a detailed explanation, as is usual with the great majority of EU legislative proposals.

38. **A project of this importance and magnitude needs to be developed openly and publicly. It potentially affects not just EU citizens, but also hundreds of thousands of non-EU citizens who may wish to travel to or reside in the EU. Information must be readily available, not just to EU institutions and national experts, but to all those affected.**

39. **It is unacceptable for a project with such cost and resource implications to be developed without a prior full impact assessment, and a full legislative explanatory memorandum.**

40. **The Government should press for greater transparency in the future development of the project, including the award of contracts.**

Legislation for SIS II

41. The legislation for the establishment of SIS II was contained in three measures proposed by the Commission in May 2005: a Regulation concerning SIS II immigration data; a Regulation concerning access by vehicle registration authorities to SIS II data on stolen vehicles; and a third pillar Decision concerning policing and criminal law data.[33] Three different measures were necessary because any measures 'building upon" the Schengen *acquis* following its integration into the EU's legal framework had to be based upon the correct legal bases in the EU and EC Treaties: EC immigration law powers (as regards the immigration data); EC transport law powers (as regards access to data on stolen vehicles); and EU policing and criminal law powers (as regard police and criminal law data).

42. The SIS II Regulation concerning immigration data will take effect as EC law, whereas at present the current SIS remains almost entirely a third pillar measure. This will entail the direct applicability of the Regulation in national legal systems, the Court of Justice's jurisdiction in the truncated form applicable to EC immigration and asylum law,[34] and the application of EC rules and principles in other areas (such as the use of the EC budget, the rules on accountability of EC bodies, and the application of EC data protection rules).

---

32 OJ C 91/38 of 19 April 2006.

33 See respectively COM(2005)236, 237 and 230, all 31 May 2005.

34 This will mean an increase in the Court's jurisdiction in most new Member States, but a *reduction* in its jurisdiction in most old Member States, compared to the current SIS, which is essentially subject wholly to the Court's third pillar jurisdiction as set out in Article 35 TEU, which gives Member States options as to whether to confer jurisdiction upon the Court at all regarding references from their national courts. On the decisions taken by Member States, see OJ 2005 C 327/19.

43. The two EC Regulations were both subject to the co-decision procedure with the European Parliament, as well as to qualified majority voting in the Council. After an agreement at first reading between the Council and the European Parliament, both Regulations were adopted on 20 December 2006, and entered into force on 17 January 2007.[35] The third pillar Decision, which was subject to consultation with the European Parliament and unanimous voting in the Council, has been agreed in principle but was not adopted at the JHA Council meeting on 15 February 2007 because Denmark and Sweden maintained their parliamentary scrutiny reserves.[36]

44. As compared to the current SIS, the new legislation provides for the inclusion of biometric data into SIS II, as mentioned above. The new legislation also provides for revised rules on data protection. Although all six of the current categories of alert have been retained, without any additional categories being added, there have been amendments to the detailed rules applicable to four categories (immigration alerts, extradition alerts, surveillance alerts and alerts on objects).

45. As for access to alerts and the power to input alerts, the existing rules are unchanged, except for an extension of access to alerts for the national members of Eurojust, the EU prosecutors' agency, which will have power to access alerts concerning extradition, missing persons, wanted persons and alerts on objects.[37] There are also revised provisions on the system of "flagging" alerts, which allows a requested State to prevent a requested action (such as the arrest of a person) from being carried out on its territory following a hit. (QQ 231–233) Furthermore, SIS II will provide for a link between different alerts; the current SIS does not provide for this.

46. The Commission's proposals would have gone further in several respects, in particular: requiring a greater level of harmonisation regarding the grounds for issuing an immigration alert; conferring power upon the Commission to manage SIS II; providing for more detailed rules on the authorities with power to access alerts and the circumstances in which they could access them; allowing wider possibilities for the transfer of SIS II data to third parties; and setting out longer periods for retaining data in SIS II as compared to the current SIS.[38]

47. During the negotiation of this proposal, in the first half of 2006 the Austrian Presidency sought to drop most of the changes to the existing Schengen Convention rules that had been proposed by the Commission. However, the

---

35 Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ 2006 L381/1 of 28 December 2006); and Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ 2006 L381/4 of 28 December 2006). It is to the latter Regulation that we refer hereafter as "the Regulation".

36 Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II). The latest text is document 14914/06 of 12 December 2006. We have maintained our scrutiny reserve but have indicated, in accordance with paragraph 3(b) of the reserve, that ministerial agreement need not be withheld pending scrutiny. This is the Decision to which we refer hereafter as "the Decision".

37 At present Eurojust can only access alerts concerning extradition and wanted persons.

38 The final legislation simply applies to SIS II the current SIS rules regarding the period of retaining data (compare Articles 112 and 113 of the Schengen Convention, as amended in 2005, with Article 38 of the Regulation and Articles 44 and 45 of the Decision).

Council had to modify this approach in order to take account of the joint decision-making power of the European Parliament, which wanted to retain many of the changes proposed by the Commission and insert further changes of its own. The Council agreed on the legislation in June 2006, but negotiations with the European Parliament continued under the Finnish Presidency before the texts could be agreed and adopted.

48. It proved difficult for parliaments and civil society to obtain any access to texts under discussion, or to follow the progress of negotiations between the Council and the European Parliament. JUSTICE pointed out the "notorious difficulty for non-governmental organisations … to obtain up-to-date information about the current state of Commission proposals for legal instruments, such as SIS II, under negotiation in the EU Council". (p 132) The situation is complicated because when the European Parliament and the Council seek to agree on legislation at the "first reading" of the co-decision process,[39] there is no formal or even informal arrangement governing the conduct of their negotiations. (QQ 76, 128, 383, 482)

49. **The lack of transparency in Council proceedings, and in co-decision negotiations between the Council and the European Parliament, is an issue relevant to all areas of EU policy-making, and has been particularly noticeable in the negotiations on the SIS II legislation. The Government should press the EU institutions to ensure greater openness and transparency of their proceedings, and in particular to codify the procedures for co-decision negotiations. All drafts of legislation should as a general rule be published immediately.**

50. The legislation does however require regular reports and evaluations of SIS II, unlike the current SIS, where there is in practice no system of reporting to the public or evaluating its functioning. This is an improvement we welcome.

Issues concerning United Kingdom implementation

51. To date, there has been minimal public consultation or Parliamentary scrutiny concerning United Kingdom participation in the Schengen Information System. Given the direct and indirect costs of participation, (Q 22) and its potential significance for both civil liberties and the operational effectiveness of our law enforcement authorities, this is most regrettable. There will be no opportunity for such a debate when SIS II is implemented in the United Kingdom if, as the Government assert, participation in SIS II does not require any amendment of our domestic law. (Q 592)

52. **To facilitate public debate on SIS II and to ensure effective Parliamentary scrutiny of United Kingdom participation in the project, the Government should undertake to publish regular reports on our preparation for SIS II, and on the planned and actual impact on the United Kingdom.**

---

[39] In the co-decision process, there are up to three readings of legislation in the Council and the European Parliament, but legislation can be agreed at any of the three readings. By 2005, legislation was agreed at first reading in over two-thirds of cases. The readings under the co-decision process are not comparable to readings under the Westminster Parliamentary process.

CHAPTER 3: HOW THE SYSTEM WORKS IN PRACTICE

Data and supplementary information

53. The SIS currently stores only "alphanumeric" data (letters and numbers), comprising (as regards individuals) data on:

- names, including aliases;
- sex and "objective physical characteristics";
- date and place of birth;
- nationality;
- whether the persons are armed or violent;
- the reason for the alert; and
- the action to be taken.[40]

54. Very often these details are not enough to give the authorities the information they need, and from the start it was realised that a system was needed for the supply of supplementary information. Each Member State holds this information on persons who are the subject of its alerts on SIS in a national database known as SIRENE (an acronym for Supplementary Information Request at the National Entry) under the control of a national SIRENE bureau, and the information on all these databases is accessible upon request to law enforcement agencies in all Member States.

55. SIRENE, though an essential feature of the SIS system, without which it could scarcely function, had no mention in the 1990 Convention, and originally had no legal base. There are now provisions requiring each Schengen State to designate a national authority—its SIRENE bureau—to be responsible for the exchange of all supplementary information, and operating in accordance with a manual—the SIRENE Manual—published by a Management Authority. The SIRENE bureau is responsible for holding supplementary information in relation to all its own national entries and making it available to the bureau of other Schengen States.

BOX 2

SIRENE UK — the United Kingdom gateway to the SIS

When SIRENE UK is activated, every routine Police National Computer (PNC) check will automatically carry out a check of the SIS via a seamless link. This will allow UK law enforcement officers to locate criminals, missing persons and stolen property from other countries.

At the same time, key information from the PNC will be available to law enforcement officers across Europe through the SIS. This increases opportunities to deal with cross-border crime and extends the reach of UK law enforcement across Europe.

When PNC alerts a law enforcement officer that a SIS match has been made, the text will inform them what action to take and to contact the SIRENE UK bureau. The bureau is housed by the Serious Organised Crime Agency. It will carry out all international communication relating to the SIS and will hold, or can obtain, extra information on the alerts on the SIS. Additionally, the SIRENE UK bureau can assist in the gathering of information in other countries and tracing fugitives from justice.[41]

---

40 Article 94(3) of the Convention.

41 Source: Serious Organised Crime Agency.

56. The SIRENE system has in the past been criticised for secretiveness; for a long time the SIRENE Manual was not published. However the Manual has now been revised and published.[42]

Categories of data

57. As between the SIS and SIS II, the main development as regards the categories of data to be stored in the system is the addition of biometric data, in particular fingerprint and photographic data, but probably also in due course DNA profiles and retina scans.[43] Such data can be used in two different ways, and the SIS II legislation distinguishes between them:

- a "one-to-one" search, using the data to confirm identity, for example by comparing the fingerprints of the person purporting to be Joe Bloggs only against the fingerprints in SIS II registered as being those of person also called Joe Bloggs);[44] and
- a "one-to-many" search, where the data is used to identify a person by comparing his fingerprints with all other fingerprints in SIS II.

58. A number of our witnesses were particularly concerned about the risks of inaccuracy which could result from one-to-many searches. Dr von Pommer Esche from the Police Intelligence Service of the German Federal Data Protection Office expressed concern about the reliability of biometrics when used for investigative purposes: "… if the Schengen Information System was not used for control purposes only it would change its character to a kind of investigative tool or method. That would be a new quality and in the long run if Member States insist on that possibility … then we must reconsider additional safeguards." (Q 299) For the Home Office Mr Rejman-Greene, a senior biometrics adviser, thought that with the rapid expansion of the database to many tens of millions of records, a necessary safeguard would be to ensure that the process was harmonised across Member States to an adequate standard: "We also have to bear in mind that each individual country will have their own standards and ways of enrolling people into a system and what needs to be checked is that that is being done across equivalent quality levels so that we do not get undue numbers of errors …" (Q 48) However, evidence from the Department for Constitutional Affairs (DCA) suggests that the Commission will be recommending only minimum standards, rather than fully harmonised enrolment rules. (Q 126)

59. The accuracy and reliability of biometric technology is of particular importance given its growing and widespread use in information systems. Biometric systems can only be designed to search for an acceptable degree of similarity. We were told that the technology can be set to obtain a high, medium or low success rating. As Superintendent Flynn explained, "so to actually talk about percentages [of false matches] can be quite difficult and misleading because you can actually vary the accuracy of the sensors." (Q 228) Data protection authorities such as the European Data Protection

---

42 The revised SIRENE Manual is annexed to Commission Decision of 22 September 2006 (OJ 2006 L 317/1).

43 These would however require amendments to the legislation.

44 It is possible, of course, that several persons share the name "Joe Bloggs". In that case, a comparison could take place also using the second biometric identifier (photographs), and/or other data stored on the SIS such as date and place of birth.

Supervisor also warn against a tendency to overestimate the reliability of biometrics and their use as a unique means of identification.[45]

60. The SIS II legislation permits the use of one-to-many searches only once the Commission reports that the relevant technology is available and ready.[46] Our witnesses differed as to the effect and timing of this.[47] Mr Peter Thompson, the Head of the European and International Division at DCA, pointed out that the report would itself "be subject to discussion in the Council and agreement by Council members, and also consultation with European Parliament" (Q 123); and we were told by Baroness Ashton of Upholland, the Parliamentary Under-Secretary of State at the DCA, that the Council decision would need to be unanimous. (Q 258)

61. **The SIS II legislation permits the use of one-to-many searches only once the Commission reports that the relevant technology is available and ready. The Government must press for:**

- **the Commission report to be drawn up on the basis of the opinion of independent experts;**
- **the certification by the Commission that the technology is ready, sufficiently accurate and reliable;**
- **the report to be adopted by unanimous vote of the Council after consultation with the European Parliament.**

The Government must deposit the Commission report for scrutiny, and the views of Parliament must be taken into account.

Types of alert

62. Unfortunately, we were unable to obtain many statistics on the operation of SIS. Mr Gerrit Huybreghts, a Council expert on statistics, explained to us that "it was only in 2005, because of remarks that were made in the European Parliament about secrecy in relation to the number of SIS data and because of questions from the academic world, that the Presidency took the initiative to publish yearly statistics but without giving details about the different Member States." (Q 327) He told us that delegations were sensitive about giving national data. Quite apart from that, "not a lot of statistics are made about the SIS and available at Council level … There is no large scale exercise in statistics for SIS I." (QQ 332, 333)

63. The few statistics we have seen on the numbers and types of alerts are poorly presented and insufficiently informative. However the following figures show the numbers of entries on the central database at the beginning of 2005, 2006 and 2007:[48]

---

45 Opinion of the EDPS on the draft SIS II legislation, OJ C 91/44 of 19 April 2006.

46 See Article 22 of the Regulation and Decision.

47 Home Office witnesses would be "disappointed" if the report was not produced by 2009 (QQ 579, 581).

48 Documents 8621/05 and 5239/06.

TABLE 1

Valid (unexpired) entries on the central SIS database at 00.00 hrs on 1 January

Type	2005	2006	2007
Banknotes (suspect notes)	347,773	252,442	241,062
Blank official documents which have been stolen, misappropriated or lost	348,037	403,900	386,440
Firearms	343,946	297,021	294,490
Identity papers (passports, identity cards, driving licences) which have been stolen, misappropriated or lost[49]	9,802,585	11,353,906	13,752,947
Motor vehicles which have been stolen, misappropriated or lost	1,183,191	1,469,378	1,731,115
Trailers and caravans which have been stolen, misappropriated or lost	3,050	3,153	3,063
Wanted persons (main)(see Table 2)	818,673	882,627	894,776
Wanted persons (alias)	338,311	340,856	312,052
Total	**13,185,566**	**15,003,283**	**17,615,495**

64. The "wanted persons" are wanted for a variety of reasons.

TABLE 2

Breakdown of Wanted Persons

Article of Schengen Convention	2005	2006	2007
95 (Extradition to a Schengen State)	15,012	15,460	16,047
96 (Third-country nationals who should be denied entry)	714,078	751,954	752,338
97 (Missing persons—adults)	19,022	19,855	21,151
97 (Missing persons—minors)	17,213	19,156	21,349
98 (wanted as witnesses, for prosecution or for enforcement of judgments)	35,317	45,189	50,616
99(2) (serious criminal offences)	18,031	31,013	33,275
Total	**818,673**	**882,627**	**894,776**

The total for each year is thus the same figure as in the entry for Wanted Persons for that year in Table 1.

---

[49] In 2006 the United Kingdom Identity and Passport Service processed 290,996 reports of lost and stolen passports: 237,879 reports of lost passports, 41,830 stolen, and 11,287 in other categories, including those reported as damaged or destroyed. In 2006 298,172 replacement passports were issued. This includes those issued to replace lost or stolen documents, and also replacements following a change of name, and replacements where the original passport has been damaged but is returned with the application for a replacement. (Official Report, 31 January 2007, col. WA 55)

65. The identification of wanted persons cannot be assisted by the fact that in some countries there is no legal requirement for a change of name to be registered. In the United Kingdom a person's name is the name by which he is known by "usage and repute". In reply to Written Questions from a member of the Committee the Registrar-General for England and Wales wrote:

> "There is no government agency that is responsible for registering the change of name of individuals. There is no requirement to register a name change in order for it to become lawful. An individual may choose to make a statutory declaration or deed poll to provide evidence of their change of name.
>
> "There is no central record of all name changes. Individuals are responsible for notifying relevant agencies that they have changed their names."[50]

66. It might be argued that the collection of statistics relating to SIS II would create too great an administrative burden upon Member States. However Member States are already obliged to collect statistics on the numbers of persons refused entry at EU external borders, the grounds for refusal, the nationality of the persons refused entry and the type of border at which they were refused entry.[51] They are also obliged to collect statistics relating to visas,[52] and concerning illegal migration at external borders.[53] A Regulation requiring Member States to collect comprehensive statistics on all aspects of migration and asylum has largely been agreed between the Council and the European Parliament.[54] Member States also collect information relating to European Arrest Warrants, including information relating to the use of SIS.[55] What is obviously needed for the purpose of assessing and monitoring the working of the SIS, and SIS II, is that national statistics are collected and presented in a format that makes them comparable and relevant.

67. As is evident from Table 2, the vast majority of entries concern Article 96 alerts, i.e. unwanted aliens. A recent report by the Schengen Joint Supervisory Authority[56] on an inspection of the use of Article 96 alerts highlighted that there was an unacceptable divergence of national practices on the issuing of these alerts. As JUSTICE put it: "In some Member States expulsion decisions lead automatically to [a] SIS alert; in others a separate decision (and thus a separate verification of the necessity of [a] SIS alert) is needed. Two Member States are notorious for issuing alerts for all failed asylum seekers, other Member States do not operate such an automatic alert policy." (p.136)[57] Professor Guild also expressed concern about "the

---

50 Official Report, 29 January 2007, col. WA 15.

51 Article 13(5) of the Schengen Borders Code (Regulation 562/2006, OJ 2006 L 105/1).

52 Schengen Executive Committee Decisions, OJ 2000 L 239/173 and 196.

53 Schengen Executive Committee Decision, OJ 2000 L 239/176.

54 See Council document 17005/06, 22 Dececember 2006.

55 See most recently Council document 9005/5/06, 18 January 2007.

56 The report was published on 20 June 2005. The Joint Supervisory Authority (JSA), set up under Article 115 of the Schengen Convention, supervises the technical support of the SIS. The Information Commissioner has observer status which has allowed him to participate in meetings of the JSA discussing data protection issues arising from the move to SIS II. (p 39)

57 The German automatic alert policy on failed asylum seekers is the basis of the litigation referred to in paragraph 74 below.

extraordinary flexibility of the criteria on the basis of which somebody may be registered in the SIS, and the very wide degree of discretion which is left to a particular Member State official to insert someone's information into the SIS." (Q 98) Problems with these alerts are compounded by what Mr Huybreghts referred to as the "very poor quality as regards [statistics on] Article 96 data". (Q 337)

68. **Full and clear statistics must be published at regular intervals, and should include:**

- **the number and type of alerts per Member State;**
- **the number and type of hits per Member State;**
- **the use of the SIRENE system for each type of supplementary information exchanged by each Member State; and**
- **actions taken following a hit for each type of hit and for each Member State**.

69. **There must be harmonisation of statistics to ensure consistency and comparability between EU and national statistics on SIS II relating to extradition requests, visa refusals, refusals of entry at the border and refusals to grant or renew residence permits.**[58]

70. As for the use of SIS II data to refuse entry to persons, as we pointed out in a previous report, the wide divergence between differing national approaches to listing a person on the current SIS to ban them from entry cannot be justified.[59] It is therefore unfortunate that, contrary to the Commission's proposals, there has been no attempt to harmonise the substantive rules for listing persons to be denied entry; although at least the issue is due to be reviewed in the future. There has been some procedural harmonisation, as all Member States can ban a person from entry only following an individual assessment, and must give that person the right to appeal. The latter right is linked to the "right to information", a data protection right considered further in chapter 6.

71. **We welcome the procedural harmonisation concerning immigration alerts contained in the legislation, but there should also be harmonisation of the substantive rules for listing a person. There should be a requirement to publish in the Official Journal a summary of the different national laws and practices concerning the creation of an immigration alert.**

72. **The forthcoming review of the grounds for listing an immigration alert should also examine how well the right to appeal is secured in practice, and whether there is a need to address the timing of the right to appeal, and its link with the right to information.**

Family members

73. A particular issue in this context is the application of SIS II to family members of EU citizens. Such persons, even when travelling with the EU

---

[58] This might well be a task for Eurostat, the European Statistical Office in Luxembourg, but we have received no evidence on this.

[59] *Illegal Migrants: proposals for a common EU returns policy*, 32nd Report, Session 2005–06, HL Paper 16, paragraph 134.

citizen who is their relative, can be denied entry to and residence in other Member States pursuant to EU free movement law, but only if they represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society.[60] Furthermore, EU free movement law sets out detailed procedural rights.[61] The standard set by the current SIS rules, and the future SIS II rules, is much less strict.

74. The conflict between these two sets of rules was addressed in a judgment of the Court of Justice in January 2006.[62]

BOX 3

The ECJ Judgment in *Commission v Spain*

An Algerian man, an "alien" for Schengen purposes, was married to a Spanish woman. They lived in London, and hence outside the Schengen area. Normally the husband would have had a right of entry into a Member State under the Directive on free movement of persons. Under the Directive, entry could be refused only if there was a genuine and serious threat to the interests of society. When the couple applied to the Spanish Consulate in London for a visa for Spain, this was refused on the ground that he was the subject of a SIS alert issued by Germany. The Court ruled that the presence of a SIS alert was not on its own enough to justify refusal of entry. To satisfy the requirements of the Directive, Spain should have sought further information through the SIRENE bureau to judge whether the alert was based on material showing that the Algerian national was in fact a genuine and serious threat to the interests of society.

75. The Commission had proposed removing family members of EU citizens from SIS II, a position also supported by the Meijers Committee and ILPA, (Q 93)[63] but the Council and European Parliament decided to retain them, subject to an express reference to the priority of EC free movement law and the use of the SIRENE system. JUSTICE told us: "We cannot see the need to treat differently EU citizens (for whom an SIS alert cannot be issued) and third-country nationals with free movement rights (who will typically be spouses or close family members of an EU citizen) … it smacks of an unjustifiable discrimination …" (p 138)

---

60 See in particular Cases: 41/74 *Van Duyn* [1974] ECR 1337; 67/74 *Bonsignore* [1975] ECR 297; 36/75 *Rutili* [1975] ECR 1219; 30/77 *Bouchereau* [1977] ECR 1999; 115/81 and 116/81 *Adoui and Cornuaille* [1982] ECR 1665; C–348/96 *Calfa* [1999] ECR I–11; C–100/01 *Olazabal* [2002] ECR I–10981; C–482/01 and C–493/01 *Orfanopolous and Olivieri* [2004] ECR I–5257; and judgment of 27 Apr. 2006 in Case C–441/02 *Commisson v Germany*, not yet reported.

61 See in particular: *Rutili* (ibid); *Adoui and Cornuaille* (ibid); *Orfanopolous and Olivieri* (ibid); *Commisson v Germany (ibid); and Cases:* 48/75 *Royer* [1976] ECR 497; 98/79 *Pecastaing* [1980] ECR 691; 131/79 *Santillo* [1980] ECR 1585; C–297/88 and C–197/89 *Dzodzi* [1990] ECR I–3763; C–175/94 *Gallagher* [1995] ECR I–4253; C–65/65 and 111/95 *Shingara and Radiom* [1997] ECR I–3343; C–357/98 *Yiadom* [2000] ECR I–9265; C–459/99 *MRAX* [2002] ECR I–6591; and C–136/03 *Dorr and Unal* [2005] ECR I–4759. The substantive and procedural rules on the refusal of entry or expulsion of EU citizens and their family members have recently been revised in the Directive on EU citizens' free movement rights (Articles 27–33 of Directive 2004/38, OJ 2004 L 229/35, applicable from 30 April 2006).

62 Case C–503/03 *Commission v Spain,* 31 January 2006

63 See also the written evidence of the Meijers Committee, paragraph 5b, p 14.

76. **The United Kingdom is particularly affected by the application of the current SIS, and SIS II, to the family members of EU citizens. A British family which includes a third-country national subject to a SIS or SIS II alert will not be able in practice to travel to the Schengen area. This is justified if the third-country national has committed crimes sufficiently serious to justify exclusion under EC free movement law, but not otherwise. The application of SIS and SIS II rules needs to be monitored closely to ensure that they are being correctly applied.**

77. SIS II will provide for the direct exchange of the full text of European Arrest Warrants, not just a summary of the data in each EAW as at present. The Crown Prosecution Service (CPS) told us that between January 2004 and August 2006, since the EAW had been functioning, they had issued a total of 307 EAWs in the United Kingdom on behalf of EU partners which had led to the arrest of 172 suspects; they estimated that their EAW caseload had doubled between 2005 and 2006. Due to the increased effectiveness of the SIS (and in future, SIS II) in determining whether an extradition request or EAW had been issued in respect of a particular individual, the United Kingdom's participation in SIS II would be likely to result in a doubling or tripling of the workload of the CPS and the Serious Organised Crime Agency (SOCA). (QQ 208, 213, 217) However, it appears from the evidence of Joan Ryan MP, the Parliamentary Under-Secretary of State at the Home Office, that no funding has yet been agreed to cover this; indeed the issue seems barely to have been considered. (QQ 589–591)

78. **The Home Office should start planning for the inevitable increase in the resources needed by the Crown Prosecution Service. The resources should be agreed in sufficient time so that the effectiveness of the Crown Prosecution Service in issuing and executing extradition requests and European Arrest Warrants is not reduced.**

CHAPTER 4: MANAGEMENT OF THE SYSTEM

79. The current SIS is at present managed by France.[64] The Commission initially proposed that it should itself be responsible for management of the SIS II system.[65] However the idea of management by the Commission was unpopular with some Member States. Mr Sweet told us that the lack of trust in the Commission arose in part from the technical difficulties the Commission had had in delivering the programme, but also from "the extent to which those delays undermined Member States' confidence more generally in the Commission's ability to manage the system as a whole." (Q 36) It was therefore decided that a Management Authority should ultimately be responsible for the operational management of the Central SIS II. A Joint Declaration of the Commission, the Council and the European Parliament appended to the Regulation and Decision commits those institutions to having the Management Authority fully active within five years.

80. During this five-year transitional period, responsibility for the management lies with the Commission, but it may delegate that task to national public-sector bodies in two different countries.[66] Under the terms of the legislation, this delegation must "not adversely affect any control mechanism under Community law, whether of the Court of Justice, the Court of Auditors or the European Data Protection Supervisor".[67] In fact it appears that, as part of the overall agreement on the SIS II legislation, the Commission has already agreed to delegate management of SIS II during the transitional period to France and Austria, which are responsible respectively for the main site in Strasbourg and the back-up site in Sankt Johann im Pongau.

81. One particular problem about the transitional period is that, despite the assertions in the legislation concerning the accountability mechanisms of EC law, the legislation establishing the EDPS limits his jurisdiction to data processing carried out by the EC institutions.[68] There is no provision permitting the EDPS to supervise data protection in Member States to which the Commission has delegated its powers. This means that the EDPS cannot take decisions concerning the processing of SIS II data in the Member States to which management has been delegated, or refer disputes to the Court of Justice.[69] Mr Thompson from DCA told us: "… we are content with the arrangements that the EDPS cannot bring proceedings under the Third Pillar and, indeed, the EDPS itself has never had powers where it could actually initiate proceedings against Member Sates." The reason for his lack of concern was that, in his view, proceedings were much more likely to be initiated at Member State level where national supervisory authorities (in this country, the Information Commissioner) could take action. (Q 117) We are not persuaded that this is a satisfactory alternative; this in our view is one more reason why the Management Authority should take over as soon as possible.

---

64 See Article 92(4) of the Schengen Convention.

65 Article 12 of the proposed Regulation and proposed Decision, respectively COM(2005)236 and 238.

66 Article 15 of the Regulation and Decision.

67 Article 15(7) of the Regulation and Decision.

68 Regulation 45/2001 (OJ 2001 L 8/1).

69 See Articles 46 and 47 of Regulation 45/2001, ibid.

82. We were told about five possible options concerning the future Management Authority. The Authority could be operated by the Commission, by Frontex (the EU's border control agency), by Europol, by one Member State on behalf of all of them, or by a new body to be established. Mr Faull told as that there would be "a major impact assessment on the long-term management of SIS II" which would also encompass "the other large-scale IT systems that have been created in the justice, freedom and security area." (Q 415)

83. The Commission, despite its initial proposal that it should manage SIS II, and despite its current role managing Eurodac (the EU system for comparing the fingerprints of asylum-seekers), does not regard the management of large-scale information systems as one of its core functions. (Q 415) We agree that an essentially operational task like the management of information systems is not easily reconciled with the Commission's duties under Article 211 of the EC Treaty,[70] and is likely to be better performed by a separate agency. The question remains whether the task should be taken on by one of the EU's existing agencies, or by a dedicated agency. Professor Kees Groenendijk, giving evidence on behalf of the Meijers Committee, was suspicious that the underlying rationale for creating a new agency might be to put it out of reach of the Community "rules of remedies, liabilities, and the general rules on transparency …" (Q 82) Mrs Laura Yli Vakkuri who, when she gave evidence to us during the Finnish Presidency, was Chair of the Schengen Acquis Working Party, said that the preference of the Presidency would be for an independent agency. (Q 494)

84. Management by an existing agency might avoid the likely delays and costs of creating an entirely new agency. However, it is unlikely that such delays and costs would be significantly reduced by assigning the management of SIS II to either of the two obvious candidates, Frontex or Europol. Frontex does not even have access to SIS data, nor will it have access to SIS II data under the governing legislation. Europol has only recently established its own information system, after extensive delays. Neither agency has sufficient relevant expertise in managing large-scale information systems. In the case of Europol there might be a conflict of interest, or at least a perception of one, between its role as a user of the service and as a service provider, particularly since it is supposed to have access only to limited categories of data.

85. Furthermore, both agencies have specialised functions of their own: Frontex has the first pillar function of assisting Member States to enforce external border controls, while Europol has the third pillar role of assisting police investigations. Europol has no direct involvement in the judicial aspects of the SIS (transmitting extradition or EAW requests, and requesting witnesses and evidence for trial purposes). Mrs Yli-Vakkuri questioned whether it was even legally possible for a first pillar agency to process third pillar information, or conversely for a third pillar agency to process first pillar information. (Q 494)

86. The planned Visa Information System (VIS), which will store information on all applications for short-term visas to visit the Schengen States, is likely to develop into a system even larger than SIS II. (Q 96) The intention is that a

---

[70] Article 211 requires the Commission to ensure that the provisions of the Treaty and the measures taken pursuant to it are applied; to formulate recommendations and deliver opinions; to have its own power of decision under the Treaty; and to exercise powers conferred on it by the Council.

dedicated agency should be set up for the management of VIS. It appears that discussions have already taken place to link the VIS and the SIS II, which complicates decisions over the future management of such large-scale European databases. (QQ 403, 420, 511)

87. Whatever is eventually decided, the legislation to establish the Authority must set out clear rules as regards the responsibility of the Commission, which is empowered to adopt many implementing rules governing the operation of SIS II, and the role of the Authority managing the system. It is also important to ensure that Member States' governments, parliaments and the public are able to scrutinize the management of SIS II effectively, and that the Authority is fully accountable for its activities. This would be even more important if, as suggested, the Authority also has responsibility for the Visa Information System, along with responsibility for other information systems or related functions, and if the EU develops the principle of "interoperable" information systems.

88. **The Government should press for the establishment as soon as possible of a dedicated Management Authority for the Central SIS II. The legislation setting it up must provide for:**

- **the Authority to have the required technical expertise in overseeing and operating large-scale information systems;**
- **the Authority to be required to publish full and clear statistics at regular intervals;**[71]
- **the Authority to be subject to effective scrutiny, including by the Court of Auditors;**
- **clear differentiation between the tasks which remain the responsibility of the Commission, and those delegated to the Authority;**
- **clear lines of accountability.**

89. Questions also arise in relation to the accountability of the Authority before the courts. There may be differences depending on whether the Authority is carrying out duties under the first or the third pillar. It should be made clear to what extent Community and national courts will have jurisdiction in proceedings brought against the Authority in the first or third pillar, for example where a data subject alleges a breach of confidentiality.

90. **The Government should ensure that individuals affected by the actions of the Management Authority are not left without an effective recourse to justice.**

---

[71] We do not believe that the requirements of Article 50(3) of the Regulation and Article 66(3) of the Decision go far enough. We explain in paragraph 68 above what these statistics should include.

CHAPTER 5: ACCESS TO DATA

91. The provisions on access to SIS II data specify broadly that the authorities responsible for border control or police checks, along with judicial authorities, can access the data. It will be possible for authorities responsible for issuing visas and for considering applications for visas or residence permits[72] to search SIS II immigration data.[73] These provisions simply copy the rules governing the current SIS, and can be compared with the Commission's more ambitious proposals to set out in more detail the precise circumstances in which different national authorities could have access to different types of SIS II data.

92. The common rules of the Regulation and Decision on data processing provide for restrictions on the copying of SIS II data and on access to and use of SIS II data other than for the purposes of checking for the specified alerts and taking action following a hit. However, unlike the first pillar Regulation governing immigration data, the third pillar Decision, dealing as it does with police and judicial cooperation in criminal matters, allows the further use of data for other purposes, where this is "linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence". Prior authorisation from the Member State issuing the alert must be obtained for this purpose.[74] This is not permitted under the current SIS rules.[75]

93. However Superintendent Flynn told us that in practice, because of the limited descriptive detail in a Schengen alert, the SIS database did not lend itself readily to investigative purposes; there were much fuller and more reliable databases and partnerships in place for the exchange of information for those purposes. (Q 240) The provision on the further use of data may therefore be little used, at least for the present.

94. It would have been desirable for Member States to be required to indicate in what circumstances they would consent to *other* Member States' further processing of SIS II data. Otherwise, the use of SIS II data as an investigatory tool, which a number of our witnesses objected to in principle, would be taking place without effective public knowledge or accountability.

95. **In order to ensure accountability, we believe that all Member States should report on the circumstances in which they will allow further processing of SIS II data, and when they will permit other Member States to process further SIS II data which they have entered.**

96. The common rules also require, for the first time, the publication in the Official Journal of a list of the national authorities authorised to search SIS II data, and for what purposes.[76] We were sent by the Home Office a list of the United Kingdom authorities which would have access to SIS II, but were asked to treat it as confidential. Accordingly we do not include it with the published evidence. Mr Mike Fitzpatrick, the Home Office SIS Programme

---

72 i.e. the embassies and consulates of all Schengen States.

73 Article 27 of the Regulation and Article 40 of the Decision.

74 Article 46(5) of the Decision.

75 See Articles 101 and 102 of the Schengen Convention..

76 Article 31(8) of the Regulation and Article 46(8) of the Decision.

Director, did however explain that most of the 80 United Kingdom authorities were constabularies. (Q 13)

97. We are concerned that this information is treated as classified. From the perspective of the person whose data is stored it is crucial to be able to determine exactly who decides which personal data is stored, and for what reason it is stored. Equally, it is important to be able to determine exactly who has access to that data, and for what purpose. This was strongly suggested by Mr David Smith, the Deputy Information Commissioner. (QQ 175, 178) The jurisprudence of the European Court of Human Rights makes clear that an interference with private life, which any storage of personal data on an information system amounts to, can only be justified on grounds of the public interest if the rules governing such interference are sufficiently detailed and accessible to the public.[77]

98. We believe that this information should currently be available as regards all Member States. In particular, it is inexcusable that the Government do not feel able to make public which United Kingdom authorities will be able to access SIS II data in the future. This is all the more perplexing given that this information will have to be published once SIS II is up and running. We cannot imagine how publication of this data could restrict the operational effectiveness of law enforcement authorities in particular cases, or in general.

99. **We welcome the provision requiring the publication of information on which authorities have access to SIS II data, and for what purposes. There is no reason why such information could not be published already in respect of access to data held in the current SIS.**

100. **The Government should now publish:**

- **the list of those authorities which will have access to SIS II data;**
- **the purposes for which they will have access;**
- **the list of those authorities which will be able to input data into SIS II; and**
- **the circumstances in which they will be able to do so.**

Access to immigration data for asylum purposes

101. One particular issue that arose during discussion of the SIS II immigration data Regulation is the question of United Kingdom access to (and input of) alerts for asylum-related purposes. We discuss this in chapter 7, but there is an underlying issue as to whether in any Schengen State asylum authorities should have access to SIS data at all. It appears from the evidence that so far only Austria gives asylum authorities access to the SIS. (Q 359)

102. The Commission had proposed that authorities should have access to data on persons in the context of an asylum procedure in order (i) to implement arrangements for the exchange of information under the Dublin Regulation[78]

---

[77] See generally, for instance, *PG and JH* v *United Kingdom* (Reports 2001–IX), *Peck* v *United Kingdom* (Reports 2003–I) and *Perry* v *United Kingdom* (Reports 2003–IX). As regards databases in particular, see *Amann* v *Switzerland* (Reports 2000–II), *Rotaru* v *Romania* (Reports 2000–V) and *Segerstedt-Wiberg and others* v *Sweden*, judgment of 6 June 2006.

[78] Council Regulation (EC) 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (Dublin II), OJ 2003 L 50/1

and (ii) to decide upon the merits of the application in the case of persons listed for denial of entry for crime-related reasons.[79]

103. Both of these suggestions are problematic in the absence of full information which would allow an asylum authority to make an informed and lawful decision. Additional information is needed to determine, in the first case, whether the detailed criteria for allocation of responsibility under the Dublin Regulation are met. In the second case, asylum authorities must be satisfied that the detailed rules concerning the question of exclusion from refugee status on the grounds of criminal activity, or suspicion thereof are complied with. It would not be right for an asylum application to be rejected without full information being exchanged between Member States.

104. It would be possible to address this issue either by providing expressly for the exchange of supplementary information through the national SIRENE bureaux following an asylum-related hit in the SIS II legislation, or by providing for a mechanism for the exchange of such information in the EC's asylum legislation. But neither the SIS II legislation nor the EC's asylum legislation addresses the issue sufficiently.[80]

105. If the United Kingdom asylum authorities were ultimately given access to this information, there would be a particular difficulty for the United Kingdom in providing information which might be used in determining asylum applications in other EU States by persons whose deportation from the United Kingdom was deemed to be conducive to the public good, or by members of their families.[81] The discretion of the Secretary of State in those cases is absolute, and reasons for the deportation are never given. If such persons were listed in alerts placed on SIS II by the United Kingdom, or their data otherwise exchanged, the Government might be forced to disclose the reasons for their deportation.

106. **Access to SIS II data (or data in the current SIS) by asylum authorities, to determine responsibility for an asylum application or to decide on the merits of an application, must be subject to detailed safeguards ensuring a full exchange of relevant information following a hit. It is not enough simply to note that there is an alert against a person.**

Europol

107. We received evidence on the SIS II project from Mr Daniel Drewer, Europol's Data Protection Officer. Although Europol in principle has had access to certain SIS alerts since October 2006, Mr Drewer told us that in practice access was still waiting for technical implementation. (Q 446) The question which arises is the purpose of Europol's access to this data, since the SIS was established (and SIS II is being established) for the purpose of providing information in order for law enforcement or immigration authorities to take action following a hit on an alert. But Europol has no power to take any action based on the alerts which it accesses.

---

79 See COM(2005)236, Article 18, and Explanatory Memorandum.

80 The rules on exchange of information on asylum applications between Member States (Article 21 of Regulation 343/2003) do not clearly address the issue of the transfer of such information.

81 Section 3(5)(b) and (c) of the Immigration Act 1971.

108. Mr Drewer told us that if there is an alert, Europol will contact the Member State concerned and ask for permission to use the alert and, if necessary, ask for supplementary information. "The information that Europol will get from the Member State that has been activated by our Schengen alert will be considered by Europol as a Member State contribution to Europol's system, so it is no longer Schengen information … and from then on we handle it according to Europol's Convention." (QQ 450, 458). Thus Schengen information becomes Europol information. This information could, under the terms of the Europol Convention, be transferred to third states or third parties with which Europol has agreements in place for the exchange of personal data. Europol has operational agreements in place with Canada, Croatia, Eurojust, Iceland, Interpol, Norway, Switzerland and the United States (Q 462). In limited circumstances information can be exchanged in the absence of such an agreement. (QQ 466, 467).

109. The witnesses from the Meijers Committee expressed concern about the possibility that information stored in SIS II would find its way to third countries. Such transfers of SIS data are not allowed in the SIS II legislation.[82] They were particularly concerned about the possibility of such information falling into the hands of the security services, because this meant losing control of how the information was used. (Q 98)

110. Europol has a legal obligation to keep reports on any retrieval of personal data. (Q 446) We believe that Europol should indicate in its annual reports how often it has accessed SIS data, and what use has been made of that data, **and we so recommend.**

[82] See Recital 18 and Article 54 of the Decision.

CHAPTER 6: DATA PROTECTION AND DATA PROCESSING RULES

111. It will be clear from what we have said that the SIS holds a large quantity of information for the sole purpose of exchanging it between the authorities of the Member States. SIS II will hold a great deal more (and more complex) information for exchange between still more States. Almost by definition, that information should be subject to a single, clear and robust regime for the protection of personal data. What we have is the exact opposite. In the words of Mr David Smith, the Deputy Information Commissioner, "this area goes completely against [making the law clear and accessible], because there is such a myriad of legal instruments … individuals whose data may appear in the system … will have real difficulties exercising their rights." (Q 160)

112. The rules on data protection and data processing in the immigration data Regulation and the third pillar Decision on cooperation in criminal law and policing have almost as many differences as they have similarities.[83] Thus in the Regulation there is a "right to information" (the right of a person to know that a file with his personal data has been established, along with who has established the file and for what purpose) that has no parallel in the Decision.[84] Conversely, the Decision has provisions for the sharing of passport data with Interpol, and regarding the applicability of the Council of Europe Data Protection Convention,[85] that have no parallel in the Regulation.[86]

113. In respect of all types of alert, there is a right for individuals to access the personal data held on them in SIS II, although access must be refused "if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedoms of third parties".[87] Everyone has the right to have inaccurate data corrected or unlawfully stored data deleted, and the legislation imposes time limits concerning requests for access, correction or deletion. Of course, the right to correction or deletion cannot be effectively exercised unless the right of access is first granted. An individual will probably not even be aware that he has an interest in exercising a right of access unless he knows that his personal data is held on SIS II and knows of the consequences of this, pursuant to the "right to information" for individuals—a right which, as we have pointed out, does not exist under the Decision.

114. As for the role of data supervisory authorities, national authorities with the powers referred to in general EC data protection legislation must monitor the lawfulness of the processing of SIS II data on their territory and its transmission from that territory, along with the processing of supplementary information via the SIRENE system. The EDPS will perform the same function for the Management Authority; during the transitional period, the Commission must ensure that the EDPS can exercise his tasks in respect of national public-sector bodies. The EDPS and the national authorities will

---

83 Articles 40–47 of the Regulation and Articles 56–63 of the Decision.

84 Article 42 of the Regulation.

85 Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

86 Articles 55 and 57 of the Decision.

87 Article 41(4) of the Regulation, Article 58(4) of the Decision.

cooperate in the exercise of their supervisory tasks. However, as noted above, the EC legislation establishing rules for data protection in the EU institutions does not confer such powers on the EDPS.

115. Further complexity results from the application of general data protection legislation to SIS II, on top of the specific data protection rules in the SIS II legislation. The immigration data Regulation, being a first pillar instrument, is subject to the EC Data Protection Directive 95/46, while the third pillar Decision is not. The Decision requires instead the application of the Council of Europe data protection Convention. But in the meantime, the Commission has proposed a Framework Decision on the protection of personal data in the field of policing and criminal law (the Data Protection Framework Decision, or DPFD). A Declaration adopted along with the SIS II Decision indicates that the general rules in the DPFD, once adopted, will apply to SIS II instead of the Council of Europe rules. However, the Framework Decision has not yet been agreed, much less adopted.

116. As an illustration of the complexities involved, it is not clear which rules (whether the ones in the DPFD, once it is adopted, or the specific rules in the SIS II Decision) will prevail where they conflict, or when a matter is regulated only under one instrument. We have asked a number of witnesses how potential conflicts are to resolved, and have received as many answers as there are witnesses.

117. For the DCA, Mr Thompson told us that his understanding was that "SIS II rules apply in addition to the DPFD rules and … would prevail" in many of the examples we cited.[88] The reason, Ms Nowell-Smith explained, is that SIS II "provides higher standards of data protection because it is dealing with a very specific type of data, in a particular database." (Q 127) However, DCA officials also reassured us that on the one example where the DPFD is stronger (i.e. the right to information, which is not provided for in the SIS II Decision), it would trump SIS II. (Q 141) The Minister, Baroness Ashton, confirmed this. (Q 255) But Dr von Pommer Esche seemed to think differently (Q 286): "There is the intention of the legislator that there should not be a right to information in the field of Schengen. That means that the general rule cannot replace the missing regulation in the SIS Decision." (Q 286). It would be unfortunate if the only way to resolve conflicts concerning the interpretation of these data protection rules was by seeking a ruling from the Court of Justice, since limitations in the Court's jurisdiction may cause difficulties.

118. Another instrument with equally complex, but different, data protection provisions is the 2005 Prüm Convention on cross-border cooperation against crime, terrorism and illegal immigration. This is not yet part of EU law, but the seven States party to it[89] are determined that it should become EU law as soon as possible.[90] The Rt Hon Geoff Hoon MP told this Committee on 12 December 2006 that the Government is now "seriously considering

---

88 Q 127 with regard to transfer of data to third states; Q 135 with regard to time limits for storage of data; Q 138 with regard to further processing.

89 Austria, Belgium, France, Germany, Luxembourg, Netherlands and Spain.

90 Six States (Italy, Portugal, Slovenia, Finland, Sweden and Romania) have already applied to join these seven States, and all of them have joined the German Presidency in proposing for discussion at the Council on 15 February 2007 a draft Council Decision which would incorporate into EU law all the third pillar provisions of the Convention.

signing up to the Prüm Convention". This would make yet another EU instrument with potentially conflicting provisions.[91]

119. **We agree with our witnesses that the data protection regime applicable to the SIS II rules is unduly complex. There are several third pillar instruments in force or in the course of preparation which have data protection provisions which are similar to but not identical with those in chapter XII of the Decision.**

120. **The third pillar Data Protection Framework Decision should prescribe exactly which data protection rules are applicable, and which are to prevail where there is a conflict. The Government should press the Council to achieve effective harmonisation of data protection rules in the Framework Decision, and ensure that it sets a sufficiently ambitious data protection standard.**

121. We examined the proposed Data Protection Framework Decision on several occasions throughout our inquiry. A number of our witnesses expressed disappointment at the most recent texts of the proposal under discussion during the Finnish Presidency, as regards the adequacy (or even the existence) of basic data protection rights. (QQ 108, 159, 162, 288) The content of this proposal, and the timing of its adoption, are still unsettled.

122. Our witnesses also expressed concern about the degree of transparency of the negotiations. A particular concern was that the proposal was being negotiated by the Council Multi-Disciplinary Group on Organised Crime (MDG), rather than by a data protection working party. Mr David Smith referred to "lack of data protection expertise [in the MDG], questioning data protection principles which are well established", (Q 172) although DCA witnesses assured us that data protection experts were sufficiently involved. (QQ 128, 149)

123. There are variations in the degree of involvement of the data protection authorities of different States which are not to the advantage of this country. Dr von Pommer Esche from the Office of the German Information Commissioner was able to say: "In Germany it is the case that … when the Federal Government deals with matters, bills and so on, which have any kind of data protection implications then we have to be involved. We are well-informed about these kinds of bills or projects." (Q 279) Contrast Mr Smith: "We are to some extent excluded … I think there is an argument that we should be a trusted expert party … in the way that, as we understand it, some of our European colleagues are. Sometimes we find out more through other data protection authorities than we find out through government departments." (Q 163)

124. **Given that the Data Protection Framework Decision would apply to SIS II, it is not appropriate to implement SIS II until the Framework Decision has been adopted and is being implemented. The Government should seek to have this Framework Decision adopted by the summer of 2007.**

125. **Because of its importance for civil liberties, the Framework Decision should be negotiated with the maximum degree of transparency and involvement of data protection authorities at national and European level.**

---

[91] We have now begun an inquiry into the Prüm Convention.

126. A further anomaly is that, in the latest drafts, the Framework Decision will not apply to Europol and Eurojust, or to security agencies, even though they will have access to SIS II data (indeed, security authorities will be able to input data on surveillance). The data protection standards set out in the Europol Convention, the decision establishing Eurojust and the national laws governing security agencies would not necessarily meet the standard to be set by the Framework Decision, at least as regards SIS II. Whatever the solution to this question, it must be one which does not compromise the operations of security agencies.

127. **As regards SIS II, the exclusion of Europol, Eurojust and security agencies from the proposed Data Protection Framework Decision is unjustified unless equivalent data protection standards apply to these bodies.**

128. We were unable to obtain much information about the application in practice of individual data protection rights under the current SIS. The SIS II legislation provides for extensive exemptions from the right of access to data and the right of information (which, as noted above, does not even exist in the third pillar SIS II Decision), so much so that Dr von Pommer Esche even questioned whether "this right to information in practice will be of any value for the data subjects". (Q 301) The content of the right to information can only be understood by a careful reading of both the EC Data Protection Directive and the relevant provision of the SIS II immigration data Regulation,[92] and even then crucial issues, like the precise timing of the information and the extent of possible limits on the right, are unclear.

129. There are, it is true, some improvements to the data protection regime in SIS II as compared to the current SIS, such as the removal of the requirement to be on the territory of a Schengen State in order to bring proceedings, the addition of a right to information (as regards immigration data), and the addition of deadlines for administrations to act upon applications to exercise rights of access and other data protection rights. But these go little way to addressing our concerns.

130. **The Government should press for amendments to the data protection rules when they are reviewed, in particular:**

- **to provide for clearer rules on the right to information, and**
- **to limit the ability of Member States to derogate from data protection rights to those cases where national security and the operations of law enforcement authorities would be directly prejudiced.**

131. As for national data protection authorities, which will have a role in ensuring that the data protection rules in the legislation are upheld, the SIS II immigration data Regulation refers to the EC Data Protection Directive, which gives substantial powers to data protection authorities.[93] However, it is not clear whether all authorities have all of the powers referred to in the Directive, or whether in any event national authorities have the resources to supervise the application of the SIS II rules effectively.

---

92 Articles 10 and 11 of the Directive (OJ 1995 L 281/31) and Article 42 of Regulation 1986/2006.

93 Art. 28 of the Directive.

132. The SIS II third pillar Decision does not make reference at all to powers of the national data protection authorities, a fact that causes concern to this country's Information Commissioner, as Mr Smith explained: "The existing Schengen Convention … says very clearly "[supervisory authorities] shall have the power to inspect or access data in the national section of SIS". As far as we can see, that is not as clearly replicated in the new decision … In the UK we have been given a power to inspect the national section of the Schengen system and we find it hard to believe that would suddenly be taken away from us." (Q 195) While the proposed DPFD does cover this issue, this measure is of course still under negotiation.

133. **The Government should seek to ensure that the Data Protection Framework Decision requires that all national data protection authorities enjoy all of the powers referred to in the EC Data Protection Directive. The Framework Decision should also make clear that this provision applies to the SIS II Decision.**

134. **The question of adequate resources for data protection authorities to enforce EU data protection rules, and the SIS II rules in particular, should be reviewed on a regular basis.**

CHAPTER 7: UNITED KINGDOM ACCESS TO IMMIGRATION DATA

135. We have referred to our 1999 Report on *Schengen and the United Kingdom's Border Controls*.[94] That report concluded that retaining the United Kingdom's present frontier controls over passengers coming from Schengen States was not a long-term option.[95]

136. Much has changed in the last eight years. Given today's climate of international terrorism, there is no likelihood of this country's frontier controls being diminished in the foreseeable future. For the purposes of this inquiry we have therefore proceeded on the assumption that these controls will be retained, and if anything strengthened.

137. Since the United Kingdom maintains checks on its frontiers with other Member States and does not participate in the borders and visas rules of the full Schengen system, as things stand we will not have access to SIS II immigration data. At the beginning of this report we explained that the pooling of information, including immigration data, was a necessary pre-condition for the abolition of border controls. Does it follow as a corollary that the abolition of border controls is a necessary pre-condition for the sharing of immigration data? This is the question we address in this chapter. It raises questions of both law and policy.

138. As we have explained,[96] the 1985 Schengen Agreement, the 1990 Convention, and the whole of the Schengen *acquis* became part of EU law by a Protocol annexed to the 1997 Treaty of Amsterdam. The United Kingdom (and Ireland) negotiated special provisions in that Protocol (Articles 4 and 5). It was on the basis of these provisions that in 2000 the United Kingdom applied to the Council for participation in the part of the Schengen system dealing with police and criminal cooperation, and approval was granted.

139. It has been accepted as a matter of law by the legal services of the Council and the Commission, and by the Government's own legal service, that these provisions do not allow the United Kingdom to participate in the provisions concerning the alerts under Article 96 of the Convention (non-EU citizens who should be denied entry to any of the Schengen States).[97] This is the reason why the United Kingdom has never even applied to participate in those provisions. The Home Office told us that the Government accept that they have "no right to access immigration data for immigration purposes given that we have not acceded to the border control aspects of Schengen." (p 119)

140. On the question of policy, the view of the Schengen States seems to be that the United Kingdom should not have access to SIS II data when it does not participate in the entirety of Schengen; they believe that a common list of persons to be denied entry to multiple Member States only has relevance if there is freedom to travel without border checks between those Member

---

94 Paragraph 8 above.

95 Paragraph 46 of the 1999 report.

96 Paragraphs 15 et seq, above.

97 This was also the view of Mrs Laura Yli-Vakkuri, then chair of the Schengen Acquis Working Party: QQ 506–507.

States. Other witnesses have also highlighted issues of principle and proportionality. Professor Kees Groenendijk expressed doubts about the fairness of the United Kingdom using "the system against certain third-country nationals without giving the large group of third-country nationals the advantage [of free movement]." (Q 103) Professor Elspeth Guild expressed the position on behalf of ILPA in more forthright terms: "… if there is not the right of free movement without a border control there is no justification for access to a flanking measure to limit free movement, and therefore the UK should not have access to the SIS unless or until it is willing to lift its internal border controls with the other Member States." (Q 105)

141. We do not think this is true in the case of decisions on the issuing of alerts under Article 96 which are "based on a threat to public policy or public security or to national security which the presence of an alien in national territory may pose".[98] We have therefore considered whether the United Kingdom should not have access to these alerts for the purposes of policing, and for other law enforcement purposes.

142. The Government stated in their written evidence that "there may be operational merit in accessing and exchanging entry refusal data contained in the SIS II for purposes other than border control". (p 119) Mr Rob Wainwright, the head of the International Department at SOCA, agreed, and thought that "the United Kingdom, notwithstanding the fact that we are retaining our border controls … should have access to the relevant part of the Article 96 database that concerns the movement of suspects of interest to us in terms of organised crime or counter-terrorism". He said that if it were possible, technically and administratively, to differentiate within the database between information there purely for immigration control purposes and information there for the control of suspects entering the EU, then "we certainly would want to access the latter, and we have been arguing the case for a technical solution to be brought to bear as part of SIS II that can allow us to participate in that way." (Q 203)

143. This position received some support from the Commission. Mr Faull did not resile from the position that "the United Kingdom not being part of the Schengen area should not have information relating to entry for the sole purpose of regulating entry because [it] has other arrangements in place regarding entry to its territory". But he felt that the United Kingdom and Ireland had contributions to make to the overall security of the European Union, and the other Member States likewise had contributions to make to the security of the United Kingdom and Ireland. There was a general perception that "the wider security implications of some of this information need to be taken into account". And, most significantly, "by making the proper distinction between the uses to which information is put ad hoc solutions can be found".(QQ 428, 429)

144. This solution would depend on it being technically feasible for SIS II to distinguish between alerts on unwanted aliens for public policy, public security and national security purposes, and those based solely on immigration. Mr Huybreghts, when asked whether it was currently possible for the system to differentiate between these alerts, told us that it was not. (Q 375) We note however that the Commission's proposal for the SIS II

98 The parallel provision for SIS II is Article 24 of the Regulation. This is not in identical terms, but the differences do not affect our argument.

immigration Regulation assumed that such a differentiation would be possible.[99] We think therefore that there is every reason for the Government to investigate whether it would be technically feasible to devise the future system so that it can differentiate between Article 96 alerts according to the use to which the information is to be put. Moreover it seems to us plain that this is a matter that should be looked at as soon as possible, while the future system is still in its relatively early stages. It would be doubly unfortunate if a way was found of adapting the system, but too late for this to be put into practice.

145. An obvious issue which arises if the United Kingdom seeks to gain access to SIS II immigration data is the data protection standards which would apply. Clearly, it would be inappropriate (and probably unlawful) for the United Kingdom to seek access to that data unless it guarantees to uphold the same data protection standards as other Schengen Member States. Equally, this country would have to satisfy all the same procedural safeguards as the full Schengen States (such as the right of appeal against a SIS II listing, and the obligation to conduct an individual assessment) and the same data processing rules (such as the ban on the transfer of SIS II data to third countries).

146. A specific approach should be taken on access to SIS II immigration data by asylum authorities. Since the United Kingdom is a full participant in EC asylum legislation, and since SIS II could make a limited contribution, subject to the necessary safeguards discussed above,[100] to the implementation of that legislation, there is a case for United Kingdom asylum authorities having access to asylum data. But given the need to adopt separate safeguards specific to the field of asylum, it would be preferable to regulate this issue by means of detailed amendments to EC asylum legislation. This would also permit our full participation in these rules, as they would constitute an amendment to legislation in which we already fully participate.

147. The United Kingdom pays the same full contribution to the costs of the current SIS and the future SIS II that we would pay if we shared all the information on the system. (Q 28–31) This seems to us an extraordinary situation; plainly it cannot continue. We are not arguing that the United Kingdom should pay a reduced contribution, but that we should receive the information to which our full contribution entitles us.

148. **We accept, as do the Government, that the position under the Amsterdam Treaty is that the United Kingdom cannot have access to all SIS II immigration data as long as it retains its border controls. However the contribution this information can make to the overall security of the European Union needs to be taken into account. We hope that when amendments to the EC and EU Treaties are next negotiated the Government will seek to persuade our partners of the benefits, to them as well as to us, of securing amendments to the relevant provisions.**

149. **In the meantime, Ministers should persuade their colleagues from the Schengen States that police and other law enforcement bodies in the United Kingdom must have access to other Member States' immigration**

---

[99] See Article 18 of the Commission's original proposal, COM(2005)236.

[100] See paragraphs 102–107 above.

data relating to the criminality of the individuals concerned. In return, the United Kingdom would make available to other Member States its own data on individuals who are undesirable due to their criminal activity.

150. **Time is of the essence. These recommendations rely on it being technically feasible to distinguish between alerts on unwanted aliens for public policy, public security and national security purposes, and alerts based on immigration control purposes. The sooner attempts are made to resolve these technical problems, the more likely they are to succeed.**

151. **To help the United Kingdom and its EU partners in their joint fight against terrorism and serious crime, the Government must therefore press ahead with representations at the highest levels.**

CHAPTER 8: CONCLUSIONS AND RECOMMENDATIONS

General Conclusions

152. The United Kingdom is not a Schengen State and will not become one in the foreseeable future. But the Schengen Information System, and its development into a second generation system, are matters of the highest relevance to this country.

153. We believe this is well understood by the police, the prosecuting authorities, and all those involved in the combating of serious cross-border crime. They appreciate the benefits to be derived from this country's participation in the information system—benefits not just for this country, but for all the States with which we can share our information.

154. We are less sure that this is fully understood by the Government. They are content not to participate in the current SIS, and likewise content that the United Kingdom should be one of the last countries to participate in SIS II. We find this hard to reconcile with their stated commitment to fighting cross-border crime.

Background—the development of the Schengen database

155. Ministers should put more resources into the development of the national connection to SIS II. Whenever the central system is ready, the United Kingdom should be ready and able to participate as early and as fully as possible. *(paragraph 30)*

156. A project of this importance and magnitude needs to be developed openly and publicly. It potentially affects not just EU citizens, but also hundreds of thousands of non-EU citizens who may wish to travel to or reside in the EU. Information must be readily available, not just to EU institutions and national experts, but to all those affected. *(paragraph 38)*

157. It is unacceptable for a project with such cost and resource implications to be developed without a prior full impact assessment, and a full legislative explanatory memorandum. *(paragraph 39)*

158. The Government should press for greater transparency in the future development of the project, including the award of contracts. *(paragraph 40)*

159. The lack of transparency in Council proceedings, and in co-decision negotiations between the Council and the European Parliament, is an issue relevant to all areas of EU policy-making, and has been particularly noticeable in the negotiations on the SIS II legislation. The Government should press the EU institutions to ensure greater openness and transparency of their proceedings, and in particular to codify the procedures for co-decision negotiations. All drafts of legislation should as a general rule be published immediately. *(paragraph 49)*

160. To facilitate public debate on SIS II and to ensure effective Parliamentary scrutiny of United Kingdom participation in the project, the Government should undertake to publish regular reports on our preparation for SIS II, and on the planned and actual impact on the United Kingdom. *(paragraph 52)*

How the system works in practice

161. The SIS II legislation permits the use of one-to-many searches only once the Commission reports that the relevant technology is available and ready. The Government must press for:

- the Commission report to be drawn up on the basis of the opinion of independent experts;
- the certification by the Commission that the technology is ready, sufficiently accurate and reliable;
- the report to be adopted by unanimous vote of the Council after consultation with the European Parliament.

The Government must deposit the Commission report for scrutiny, and the views of Parliament must be taken into account. *(paragraph 61)*

162. Full and clear statistics must be published at regular intervals, and should include:

- the number and type of alerts per Member State;
- the number and type of hits per Member State;
- the use of the SIRENE system for each type of supplementary information exchanged by each Member State; and
- actions taken following a hit for each type of hit and for each Member State. *(paragraph 68)*

163. There must be harmonisation of statistics to ensure consistency and comparability between EU and national statistics on SIS II relating to extradition requests, visa refusals, refusals of entry at the border and refusals to grant or renew residence permits. *(paragraph 69)*

164. We welcome the procedural harmonisation concerning immigration alerts contained in the legislation, but there should also be harmonisation of the substantive rules for listing a person. There should be a requirement to publish in the Official Journal a summary of the different national laws and practices concerning the creation of an immigration alert. *(paragraph 71)*

165. The forthcoming review of the grounds for listing an immigration alert should also examine how well the right to appeal is secured in practice, and whether there is a need to address the timing of the right to appeal, and its link with the right to information. *(paragraph 72)*

166. The United Kingdom is particularly affected by the application of the current SIS, and SIS II, to the family members of EU citizens. A British family which includes a third-country national subject to a SIS or SIS II alert will not be able in practice to travel to the Schengen area. This is justified if the third-country national has committed crimes sufficiently serious to justify exclusion under EC free movement law, but not otherwise. The application of SIS and SIS II rules needs to be monitored closely to ensure that they are being correctly applied. *(paragraph 76)*

167. The Home Office should start planning for the inevitable increase in the resources needed by the Crown Prosecution Service. The resources should be agreed in sufficient time so that the effectiveness of the Crown Prosecution Service in issuing and executing extradition requests and European Arrest Warrants is not reduced. *(paragraph 78)*

Management of the system

168. The Government should press for the establishment as soon as possible of a dedicated Management Authority for the Central SIS II. The legislation setting it up must provide for:
    - the Authority to have the required technical expertise in overseeing and operating large-scale information systems;
    - the Authority to be required to publish full and clear statistics at regular intervals;
    - the Authority to be subject to effective scrutiny, including by the Court of Auditors;
    - clear differentiation between the tasks which remain the responsibility of the Commission, and those delegated to the Authority;
    - clear lines of accountability. *(paragraph 88)*
169. The Government should ensure that individuals affected by the actions of the Management Authority are not left without an effective recourse to justice. *(paragraph 90)*

Access to data

170. In order to ensure accountability, we believe that all Member States should report on the circumstances in which they will allow further processing of SIS II data, and when they will permit other Member States to process further SIS II data which they have entered. *(paragraph 95)*
171. We welcome the provision requiring the publication of information on which authorities have access to SIS II data, and for what purposes. There is no reason why such information could not be published already in respect of access to data held in the current SIS. *(paragraph 99)*
172. The Government should now publish:
    - the list of those authorities which will have access SIS II data;
    - the purposes for which they will have access;
    - the list of those authorities which will be able to input data into SIS II; and
    - the circumstances in which they will be able to do so. *(paragraph 100)*
173. Access to SIS II data (or data in the current SIS) by asylum authorities, to determine responsibility for an asylum application or to decide on the merits of an application, must be subject to detailed safeguards ensuring a full exchange of relevant information following a hit. It is not enough simply to note that there is an alert against a person. *(paragraph 106)*
174. Europol should indicate in its annual reports how often it has accessed SIS data, and what use has been made of that data. *(paragraph 110)*

Data protection and data processing rules

175. We agree with our witnesses that the data protection regime applicable to the SIS II rules is unduly complex. There are several third pillar instruments in force or in the course of preparation which have data protection provisions

which are similar to but not identical with those in chapter XII of the Decision. *(paragraph 119)*

176. The third pillar Data Protection Framework Decision should prescribe exactly which data protection rules are applicable, and which are to prevail where there is a conflict. The Government should press the Council to achieve effective harmonisation of data protection rules in the Framework Decision, and ensure that it sets a sufficiently ambitious data protection standard. *(paragraph 120)*

177. Given that the Data Protection Framework Decision would apply to SIS II, it is not appropriate to implement SIS II until the Framework Decision has been adopted and is being implemented. The Government should seek to have this Framework Decision adopted by the summer of 2007. *(paragraph 124)*

178. Because of its importance for civil liberties, the Framework Decision should be negotiated with the maximum degree of transparency and involvement of data protection authorities at national and European level. *(paragraph 125)*

179. As regards SIS II, the exclusion of Europol, Eurojust and security agencies from the proposed Data Protection Framework Decision is unjustified unless equivalent data protection standards apply to these bodies. *(paragraph 127)*

180. The Government should press for amendments to the data protection rules when they are reviewed, in particular

- to provide for clearer rules on the right to information, and
- to limit the ability of Member States to derogate from data protection rights to those cases where national security and the operations of law enforcement authorities would be directly prejudiced. *(paragraph 130)*

181. The Government should seek to ensure that the Data Protection Framework Decision requires that all national data protection authorities enjoy all of the powers referred to in the EC Data Protection Directive. The Framework Decision should also make clear that this provision applies to the SIS II Decision. *(paragraph 133)*

182. The question of adequate resources for data protection authorities to enforce EU data protection rules, and the SIS II rules in particular, should be reviewed on a regular basis. *(paragraph 134)*

United Kingdom access to immigration data

183. We accept, as do the Government, that the position under the Amsterdam Treaty is that the United Kingdom cannot have access to all SIS II immigration data as long as it retains its border controls. However the contribution this information can make to the overall security of the European Union needs to be taken into account. We hope that when amendments to the EC and EU Treaties are next negotiated the Government will seek to persuade our partners of the benefits, to them as well as to us, of securing amendments to the relevant provisions. *(paragraph 148)*

184. In the meantime, Ministers should persuade their colleagues from the Schengen States that police and other law enforcement bodies in the United Kingdom must have access to other Member States' immigration data relating to the criminality of the individuals concerned. In return, the United Kingdom would make available to other Member States its own data on

individuals who are undesirable due to their criminal activity. *(paragraph 149)*

185. Time is of the essence. These recommendations rely on it being technically feasible to distinguish between alerts on unwanted aliens for public policy, public security and national security purposes, and alerts based on immigration control purposes. The sooner attempts are made to resolve these technical problems, the more likely they are to succeed. *(paragraph 150)*

186. To help the United Kingdom and its EU partners in their joint fight against terrorism and serious crime, the Government must therefore press ahead with representations at the highest levels. *(paragraph 151)*

187. We recommend this report to the House for debate. *(paragraph 11)*

APPENDIX 1: SUB-COMMITTEE (HOME AFFAIRS)

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

Baroness Bonham-Carter of Yarnbury
Earl of Caithness
† Baroness D'Souza
† Lord Foulkes of Cumnock
† Lord Harrison
Baroness Henig
† Lord Jopling
Earl of Listowel
Lord Marlesford
† Lord Teverson
Lord Wright of Richmond (Chairman)

† from 22 November 2006

The following former members of the Sub-Committee, who were members from the start of the inquiry until the end of the Session 2005–06, were co-opted to join the Sub-Committee for the remainder of the inquiry:

Lord Avebury
Lord Corbett of Castle Vale
Lord Dubs
Viscount Ullswater

Professor Steve Peers, Professor of Law, University of Essex Centre for European Law, was appointed as Specialist Adviser for the inquiry.

Declarations of Interests:

A full list of Members' interests can be found in the Register of Lords Interests:

http://www.publications.parliament.uk/pa/ld/ldreg.htm

Interests declared by Members relevant to this inquiry

Lord Dubs

Former Director, Refugee Council, London
Former Trustee, Immigration Advisory Service

Baroness Henig

Chair of the Security Industry Authority
President of the Association of Police Authorities

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 the legislative proposals which will govern the establishment, operation and use of the second generation Schengen Information System (SIS II).

In June 2005, the Commission submitted three proposals which together form the legislative basis for SIS II: a Regulation on the establishment, operation and use of SIS II with respect to immigration matters (COM (2005) 236 final); a Decision governing SIS II for policing purposes (COM (2005) 230 final); and a Regulation giving access to SIS II data by vehicle registration authorities (COM (2005) 237 final).

The three measures put in place a revised version of the Schengen Information System (SIS)—the computerised database, operational since 1995, which enables Schengen States to exchange data on persons and objects in order to maintain security in an area without internal border. The new SIS will enable up to 30 States to connect to the System and integrate biometric data.

The package of legislative proposals for the establishment of SIS II was agreed by the EU Justice and Home Affairs ministers on 2 June 2006. All 25 Member States, plus Iceland, Norway, Switzerland and Liechtenstein will be connected to SIS II once the technical work has been completed. The System is not likely to be rolled out until late 2007. The United Kingdom and Ireland are included in the database only for the purposes of police and judicial cooperation. They are not part of the free travel zone, and hence do not have access to the immigration data in the current SIS; nor is it envisaged that they should have access to this data in SIS II.

The aim of the inquiry is to examine the interpretation and application of the SIS II provisions, including points relevant to the specific position of the United Kingdom, taking into account the planned adoption of implementing measures by the Commission. The inquiry will also look at the development of SIS II against the wider context of exchange of data on Justice and Home Affairs matters, particularly with regard to current plans on interoperability of EU databases and proposed data protection rules in the third pillar.

Written evidence is invited on all aspects of the SIS II proposals. The Sub-Committee would particularly welcome comments on:

- the decision-making process which has led to the development of SIS II, particularly the adequacy of public consultation and lack of impact assessment;
- the operational management of SIS II by the Commission, and whether the rules ensure accountability;
- the implications of including biometric data;
- the provisions allowing the interlinking of alerts;
- the criteria for listing persons to be refused entry;
- the appropriateness of including third-country national family members of EU citizens in the SIS II;

- the clarity of the rules governing collection of and access to data, including the desirability of granting access to immigration data to police and asylum authorities;
- the adequacy of data protection rules, in particular as regards data which might be transferred to third countries;
- the implications of the plans on interoperability of EU databases;
- the United Kingdom's position on the SIS, particularly the need for access by the UK to immigration data.

APPENDIX 3: LIST OF WITNESSES

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

⋆ Crown Prosecution Service (CPS)

⋆ Mr Daniel Drewer, Europol Data Protection Officer

⋆ Department for Constitutional Affairs (DCA)

⋆ European Commission, Directorate-General Justice, Freedom & Security (D-G JLS)

⋆ Home Office

⋆ Mr Gerrit Huybreghts, General Secretariat of the Council

⋆ Immigration Law Practitioners' Association (ILPA)

JUSTICE

⋆ Meijers Committee (Standing Committee of Experts on International Immigration, Refugee and Criminal Law)

⋆ Office of the Information Commissioner

⋆ Dr Wolfgang von Pommer Esche, Head of Unit, Police Intelligence Service, Federal Data Protection Office, Bonn

⋆ Serious Organised Crime Agency (SOCA)

⋆ SIRENE UK

⋆ Mrs Laura Yli-Vakkuri, Chair of Schengen *Acquis* Working Party

APPENDIX 4: LIST OF ABBREVIATIONS

A8 countries (the A8)	the ten Member States which acceded to the EU in May 2004, less Cyprus and Malta
ACPO	Association of Chief Police Officers
Article 29 Committee	the Data Protection Working Party established under Article 29 of the Data Protection Directive 95/46/EC
Article 36 Committee	a Committee of senior officials responsible for coordinating activities in the field of justice and home affairs, established under Article 36 TEU
Convention 108	Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data
CPS	Crown Prosecution Service
C.SIS	Schengen Information System, central section
DCA	Department for Constitutional Affairs
"the Decision"	Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II)
DG JLS	Directorate-General Justice Freedom and Security of the Commission
DPA 1998	Data Protection Act 1998
DPFD	Data Protection Framework Decision
Dublin Regulation	Council Regulation (EC) 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ 2003 L 50/1)
EAW	European Arrest Warrant
EDPS	European Data Protection Supervisor
EC	European Community
ECJ	European Court of Justice
EU	European Union
Eurodac	Computerised EU database for storing the fingerprints of asylum applicants
Eurojust	EU agency composed of prosecutors and judges of Member States, set up to help in the investigation of serious cross-border crime
Europol	European Police Office, set up under a Convention between Member States
Eurostat	European Statistical Office
Frontex	European Agency for the Management of Operational Cooperation at the External Borders of the Member States

G6 ministers	the ministers of the interior of the six largest Member States: Germany, France, United Kingdom, Italy, Spain and Poland
G6 meetings	the regular six-monthly meetings of the G6 ministers
ICO	Information Commissioner's Office
ILPA	Immigration Law Practitioners' Association
JHA	Justice and Home Affairs
JSA	Joint Supervisory Authority: the authority set up under Article 115 of the Schengen Convention to supervise the technical support of the SIS
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs of the European Parliament
MDG	Council Multi-Disciplinary Group on Organised Crime
Meijers Committee	Standing Committee of Experts on International Immigration, Refugee and Criminal Law
N.SIS	Schengen Information System, national section
PNC	Police National Computer
PNR Agreement	Passenger Name Record Agreement
Prüm Convention	Convention between Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration
QMV	Qualified Majority Voting
"the Regulation"	Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L381/4 of 28 December 2006)
Schengen *acquis*	The Schengen Agreement, the Schengen Convention, and all the instruments adopted under them (published in OJ L 239 of 22 September 2000)
Schengen Agreement	the 1985 Agreement between Belgium, Germany, France, Luxembourg and the Netherlands on the gradual abolition of checks at their common borders
Schengen Convention	the 1990 Convention implementing the Schengen Agreement
SIRENE	Supplementary Information Request at the National Entry
SIS/SIS I	Schengen Information System
SIS II	Second generation Schengen Information System
SIS one4all	Proposal to allow the SIS to be adapted to include the A8
SOCA	Serious Organised Crime Agency
TEC	Treaty establishing the European Community
TEU	Treaty establishing the European Union
VIS	Visa Information System

APPENDIX 5: OTHER REPORTS FROM THE SELECT COMMITTEE

Session 2005–06

Annual Report 2006, (46th Report, HL Paper 261)

Relevant Reports prepared by Sub-Committee F

Session 1997–1998

Incorporating the Schengen *Acquis* into the EU (31st Report, HL Paper 139)

Session 1998–1999

Schengen and UK border controls (7th Report, HL Paper 37)

Session 1999–2000

UK Participation in the Schengen *Acquis* (5th Report, HL Paper 34)

Session 2000–01

A Community Immigration Policy (13th Report, HL Paper 64)

Session 2001–02

A Common Policy on Illegal Immigration (37th Report, HL Paper 187)

Session 2004–05

After Madrid: the EU's response to terrorism (5th Report, HL Paper 53)

The Hague Programme: a five year agenda for EU justice and home affairs (10th Report, HL Paper 84)

Session 2005–06

Economic Migration to the EU (14th Report, HL Paper 58)

Illegal Migrants: proposals for a common EU returns policy (32nd Report, HL Paper 166)

Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm (40th Report, HL Paper 221)

Session 2006–07

After Heiligendamm: doors ajar at Stratford-upon-Avon (5th Report, HL Paper 32)

Minutes of Evidence

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

WEDNESDAY 11 OCTOBER 2006

Present	Avebury, L	Henig, B
	Bonham-Carter of Yarnbury, B	Listowel, E
	Caithness, E	Marlesford, L
	Corbett of Castle Vale, L	Ullswater, V
	Dubs, L	Wright of Richmond, L (Chairman)

Examination of Witnesses

Witnesses: Mr Mike Fitzpatrick, Programme Director, Schengen Information System Programme, Mr Jonathan Sweet, International Directorate, Home Office, Mr Kevan Norris, Legal Adviser and Mr Marek Rejman-Greene, Senior Biometrics Adviser, examined.

Q1 ***Chairman:*** Good morning, gentlemen. Thank you very much for coming to give evidence to us. We are on the record and we are being recorded for the website. We are also being televised. You will of course be sent later a transcript for you to check that you are correctly recorded. This is an inquiry into the Schengen Information System, mark II. You are the first of the oral witnesses we have received but I would like to thank you also for the written evidence which your department has provided. Do any of you want to make any opening statement?
Mr Sweet: I do not think so, thank you.

Q2 ***Chairman:*** At a recent European Parliament meeting there was concern expressed about technical problems and perhaps other problems which are leading to delays in SIS II. I am rather confused from reading the papers as to exactly what the revised timetable is now. An Estonian parliamentarian referred at a recent meeting to a delay of 15 months. There have been various dates suggested in Commission papers—the delay may be until June 2008—and even suggestions that the delay may be longer than that. Would you like to comment on this delay and in particular on what problems you think are leading to this delay?
Mr Fitzpatrick: If I may speak to the original timetable to explain the delays, as originally planned the SIS II system should have gone live in March 2007 ready for borders in the Schengen area to be dropped in October. We have been working with the Commission to understand how that might be achieved and we have worked with them to develop a realistic plan which now contemplates delivery and go live for all Member States in, I think, June 2008. That is the date that we understand to be the realistic planning assumption. It is a challenging timetable but we believe it is realistic for it to be achieved.

Q3 ***Chairman:*** It has been suggested that SIS I might be extended meanwhile to cover new Member States. Would this be possible, given the current technical limitations on SIS I? Would this require further regulation and decisions?
Mr Fitzpatrick: Given the delay to SIS II and the border dropping deadline of October 2007, one can understand the desire for an alternative to be sought. We have seen a number of proposals from the Commission and Member States to broaden the membership of SIS I plus but as yet we have not seen something which we would place a lot of faith in. At the moment, we do not think that some of the challenges which were pointed out in the inadequacies of SIS I which required the development of SIS II, such as capacity, have yet been addressed in any of the proposals we have seen.
Chairman: If any of the others wish to chip in, you are of course very welcome to do so.

Q4 ***Earl of Caithness:*** On the question of delay, do you support the claim by Poland, the Czech Republic, Hungary, Slovakia and Slovenia for compensation from the Commission and, if not, why not?
Mr Fitzpatrick: The claim for compensation would depend on who was at fault and would in many cases, especially in the countries concerned—I cannot comment on their particular state of readiness—require proof that everybody was ready. This is a collective enterprise and, while there are certainly some delays which have occurred at the Commission level between them and the contractor, there are also delays elsewhere in the delivery of the central system

in Strasbourg and also, from our perspective, some questions as to whether all Member States would have been ready to connect in March 2007 anyway.
Chairman: Incidentally, if on this or any other points, when you read your transcript, you think there is anything that needs to be followed up in writing, we would of course very much welcome that.

Q5 ***Lord Avebury:*** A number of Member States did ask for a comprehensive explanation as to the reasons for the delay and I presume that this would have been given to them in writing. If that was so, could we solicit the copies of the explanation given by the Commission and have them distributed to the Committee?
Mr Fitzpatrick: I am not aware but we will check to see if we have a comprehensive statement from the Commission. There has been reference to a submission before on the delays in the provision of the Strasbourg site, air conditioning, flooring and so forth, and mention of the contracting delays which have occurred following appeals with the letting of various contracts. The original SIS II contract which was won by H P Sterio was delayed, as was the award of the network contract for the S-test network to run SIS II.

Q6 ***Lord Avebury:*** Could you perhaps say something about the secrecy which surrounds the SIS II documents, particularly the rescheduling document 12379? Why is it necessary to conceal from new Member States and from the public what has gone wrong with SIS II? Why can there not be openness, particularly under the Finnish presidency which believes so strongly in transparency?
Mr Fitzpatrick: I am afraid I do not know the document to which you are referring specifically.

Q7 ***Lord Avebury:*** It is not the only one.
Mr Fitzpatrick: I am not aware that any documents are particularly being kept secret from Member States. We have access, as other Member States do, to the planning approach of the Commission and the documents they provide. There is no way in which they are, as far as we are concerned, kept secret or access restrained from any Member State.
Chairman: I should say that at the meeting in Brussels, which I think Lord Avebury attended, the statement by the Estonian parliamentarian reflected considerable concern both about the delay but also about the lack of transparency.
Lord Avebury: Even the chair of the Finnish committee which deals with European Union affairs was saying that she did not get all the papers. It is a pervasive climate of secrecy surrounding these particular documents which is very harmful to a complete understanding of the reasons for the delay and the methods for putting it right, which I think we should protest against.

Q8 ***Baroness Henig:*** I am switching the focus, if I may, to the United Kingdom's position, and particularly what is the timescale for the United Kingdom participation in the current SIS and why has this participation been so long delayed?
Mr Fitzpatrick: As has been previously stated, our aspiration is to join SIS II in 2009. We think we will be ready. We have put together a robust and, we think, deliverable plan to do so. It is obviously subject to proper programme delivery practices and any particular things that come about in the interim. The issue of delay, by which I take it you mean to be the lack of connection to SIS I, was caused by several factors. There have been some acts of God. Fire destroyed some equipment, but this was a complex programme put together between a number of agencies and when I joined the project last October it is fair to say that our assessment was that, at that point, SIS I connection for the UK would not have been achieved by the time SIS II would have been delivered for the rest of the Member States. We consulted with ministers who took the decision that we should concentrate our efforts now on delivering SIS II to a properly robust programme and timetable.

Q9 ***Chairman:*** Can I ask the legal adviser: do you have any comment on the progress of the case in the European Court?
Mr Norris: Do you mean the case that the UK challenges?

Q10 ***Chairman:*** Yes.
Mr Norris: These are the two cases where the UK has brought proceedings because, although we sent opt-in letters in relation to the European border agency regulation and the passport regulation, that opt-in was not accepted and we were excluded from participating in those two instruments. The written procedure has now finished in relation to those proceedings and we are waiting for a hearing date but at the moment we have no hearing date. I am unable to say when we will get a hearing or in fact a judgment.

Q11 ***Baroness Henig:*** You say you are aiming for 2009. In view of the almost certain slippage in SIS II coming on stream and the problems that newer states have come across, is that not likely to slip as well? Presumably, the slippage in the programme in terms of the European Commission point of view must affect your planning as well?
Mr Fitzpatrick: At the moment, we do not believe that further delay in SIS II being delivered by the Commission—i.e., the central system—will affect our

timetable. It is true to say that given the history of this project one cannot rule out the fact that there will be such delays that will affect it, but we believe that the programme now to deliver in 2008 is reasonably robust, if challenging, and all Member States will be connected at the point when the UK will join in 2009.

Q12 ***Baroness Henig:*** It is optimistic but deliverable?
Mr Fitzpatrick: The word I used was "challenging".

Q13 ***Baroness Bonham-Carter of Yarnbury:*** Precisely which UK authorities will have access to data in SIS and SIS II?
Mr Fitzpatrick: We have a list of 80, mostly constabularies. They are the established authorities who are able to access information on the police national computer and we will be using the same protocol for that. We will provide that in written evidence.

Q14 ***Baroness Bonham-Carter of Yarnbury:*** There seems to be disagreement over SIS immigration data, between what the UK is hoping to have access to and what the rest of the Council legal service thinks we should have access to.
Mr Norris: Yes, there has been a dispute. I have referred to the two cases where our participation in measures, described as Schengen building measures, have been disputed. In this case, it is slightly different because we did not purport to opt into the SIS II regulation and we accept that generally it is to do with providing information for Schengen immigration purposes. We do not participate in Schengen in relation to immigration. We are in a different position here. What we were pushing for in relation to the SIS II instrument was that, in so far as the asylum authorities of other Schengen Member States were being given access to Schengen immigration data for asylum purposes, the UK asylum authorities should be in the same position. Although we were not participating in the SIS II regulation, so it was not for that regulation to provide for our access to this information, nevertheless arrangements ought to be made to put UK asylum authorities in the same position as other asylum authorities for asylum purposes. Unfortunately, that was not accepted during negotiations but there was some sympathy for our position and we are now going to look to see whether there are other ways that our asylum authorities can get access to this data—for example, under the arrangements for the exchange of information in the Dublin II regulation, a regulation dealing with asylum and determining which authority is responsible for determining asylum applications.

Q15 ***Baroness Bonham-Carter of Yarnbury:*** That is being pursued?
Mr Norris: We are looking into that.

Q16 ***Chairman:*** That is what is described as access to alerts, is it, for the purpose of refusing entry?
Mr Norris: Yes. It was felt that that information would be relevant when determining which Member State had to determine an asylum application.

Q17 ***Earl of Caithness:*** Has there been an external audit to justify the cost effectiveness, efficiency and added value of SIS I and, if so, are there any lessons to be learned for the UK authorities with regard to SIS II?
Mr Fitzpatrick: A cost effectiveness study for SIS II is being done at the moment. We are compiling a business case to analyse the benefits both in terms of law enforcement operation into the UK generally and in terms of arrests. We have very useful information from other Member States about the number of alerts and the number of arrests that they are able to make through having the system in play as SIS I.

Q18 ***Earl of Caithness:*** But nothing about the efficiency and added value?
Mr Fitzpatrick: That work is ongoing at this time, before we commit finally to a contract for delivering the system.

Q19 ***Viscount Ullswater:*** Mr Norris, I want you to help me with a sort of conundrum which I see in this particular area. The UK has access to information on Eurodac which is for asylum application. That does not cause a problem in the Schengen sense, or it does not seem to. Why is the other immigration information which is part of Schengen causing such a problem to the Commission, to the Schengen countries, that they will wish to deny the UK access to this information?
Mr Norris: My understanding of their position is that they were reluctant to allow the UK to have on-line access—i.e., a SIS II terminal in the UK—to this data, even though we would only be accessing that data for asylum purposes and not immigration purposes. I think they have made it clear that if we enter into bilateral arrangements under the Dublin II arrangements to get access to this data they are not objecting to that indirect access, but what they are objecting to is the idea that the UK should have direct, on-line access to the immigration data part of SIS II.

Q20 ***Lord Marlesford:*** Why?
Mr Norris: The feeling is that, as we do not have an SIS II terminal on UK territory providing access to this data for immigration purposes, we should not be afforded on-line access for ancillary purposes like asylum. I am trying to state a case obviously that I do not support, at least to try and explain why we have had the negotiating difficulties we have had.

Q21 ***Earl of Listowel:*** We have been discussing the access by agencies in this country to SIS II. Is Her Majesty's Government confident that the appropriate agencies will be accessing this information within the European Union when it is put in place? Have you information on that, please?
Mr Fitzpatrick: There is obviously the established process for checking the use of Schengen information through the Schengen evaluation working group, which is composed of representatives from each Member State, which goes from country to country essentially checking on how the information is used in each Member State. That is essentially the assurance that each Member State relies on to ensure that this data is being used in accordance with global interests.
Mr Sweet: It is also the case, as I understand it, that the bodies in the other Member States that will have access are in fact recognised bodies which are listed in the Schengen handbook. In other words, it is not open to anybody simply to try to obtain access to it. These must be recognised bodies which are already listed in the relevant Schengen handbook.

Q22 ***Lord Corbett of Castle Vale:*** Mr Fitzpatrick, can you give us some idea of the estimated costs of participation in SIS and SIS II?
Mr Fitzpatrick: Our current estimate of the cost of implementing SIS II is £39 million. That includes subscription to the Commission's costs for SIS II which run at half a million pounds a year and that £39 million cost includes the Home Office costs and the subscription costs for delivering the system in 2009.

Q23 ***Chairman:*** Does that take into account the latest delays or not?
Mr Fitzpatrick: The delays to the SIS II system in Strasbourg, yes.

Q24 ***Lord Corbett of Castle Vale:*** 39 million is, if you like, the entry cost and there is an annual cost?
Mr Fitzpatrick: Yes.

Q25 ***Lord Corbett of Castle Vale:*** What is the annual cost?
Mr Fitzpatrick: The annual cost is half a million pounds for SIS II subscription to the Commission for its costs in running the system. There will obviously be operational costs for running the system in the UK and supporting the technology and people to manage it.

Q26 ***Lord Corbett of Castle Vale:*** Have you a figure for that?
Mr Fitzpatrick: It is in the order of about £3 million to £4 million a year. I will correct that if I am wildly inaccurate.

Q27 ***Lord Marlesford:*** Half a million pounds to the EU Commission for running SIS II, I think you said.
Mr Fitzpatrick: Yes.

Q28 ***Lord Marlesford:*** What is that based on in terms of other countries' contributions?
Mr Fitzpatrick: That is the total costs divided up pro rata, of which we pay 18 per cent.

Q29 ***Lord Marlesford:*** Pro rata to what?
Mr Fitzpatrick: Pro rata across each Member State. I cannot remember the formula. I do not know whether it is GDP or population but there is an established formula by which central costs are attributed amongst Member States and half a million is our 18 per cent proportion.

Q30 ***Lord Marlesford:*** We are paying a full subscription but we are not getting the full information? Is that correct?
Mr Fitzpatrick: Yes, that is correct.

Q31 ***Lord Marlesford:*** How do they justify denying us the information when we are paying for it?
Mr Fitzpatrick: I do not have anything to add to the answer Kevan gave earlier.
Lord Marlesford: This is an important point.
Chairman: If you have anything to add on that in writing, please let us have it.

Q32 ***Lord Marlesford:*** Have you considered reducing your half million to take account of the fact that you are not getting information?
Mr Fitzpatrick: I think it is something which we will take away and consider.
Chairman: We look forward to hearing more from you on that.

Q33 ***Earl of Caithness:*** This is following up Lord Avebury's point. He was concerned about the secrecy and lack of transparency. Can you tell us, please, why there has been no prior impact assessment, no public consultation and no explanatory memorandum by the Commission on its proposals?
Mr Sweet: I can try to answer that question, I suppose, by giving a little bit of the context and the history of it. Consultation did take place before the

implementation of SIS I. The Commission themselves provided an explanatory memorandum on the development and legal base for SIS II as part of their proposals when they tabled their proposals, those proposals outlining the need for SIS II. It is also the case that since in some respects one can regard SIS II as essentially a development of SIS I, the fundamental rationale for the system is the same now as it was when the original SIS proposal was produced. On that basis, the Commission felt that it was unnecessary to do a further impact assessment in relation to SIS II. It is true of course that during the development of their new legal base for SIS II the Commission did consult a range of interested parties and stakeholders, notably the Joint Supervisory Authority, the European Data Protection Supervisor and the Article 29 Committee on Data Protection whose views were all sought. In essence, the view is that the evolution of SIS into SIS I plus brings it closer to what will be the shape of SIS II, sufficiently enough to mean that the original impact assessment and explanatory memorandum essentially set out the rationale which still exists.

Q34 ***Earl of Caithness:*** You have already confirmed that there has been no independent audit on the cost effectiveness, efficiency and added value of SIS I; yet you would be perfectly happy to roll this forward into SIS II without any of the supporting evidence to justify it. Are you really content that that is how the Commission should proceed and that Her Majesty's Government should be a part of that decision?
Mr Sweet: We are naturally keen that the Commission should be as transparent as possible and we are amongst those who, in the relevant Council working groups, have pressed the Commission to be as open as they can be about the development of the programme and indeed about the potential problems which may have arisen in relation to the programme. We certainly subscribe to the views that were essentially set out in the Hague Programme itself about the need across the whole range of justice and home affairs issues for there to be proper evaluation and impact assessment on any proposals. It was the Hague Programme of course which did set down essentially the recognition that we needed to move increasingly to a system where there were those impact assessments and evaluations. We certainly subscribe to the view that the Commission should be as open and transparent as possible and that the Council itself should be informed of developments and changes to the programme.

Q35 ***Earl of Caithness:*** Do you think they have been?
Mr Sweet: My personal view is that they could have been more open about those arrangements.

Lord Avebury: In the memorandum by the Home Office you say that most Member States support the creation of a new cross-pillar agency to manage SIS II subject to a suitable impact assessment. Before you answer my question about the impact assessment, what stage that has reached, could you say first why the Home Office thinks that the management of SIS II by the Commission proved unpopular with Member States and particularly bearing in mind that they agreed to the Commission management of Eurodac? What specific concerns did Member States have about management by the Commission?

Q36 ***Chairman:*** Why is a workforce satisfactory when the Commission is not?
Mr Sweet: To answer one of your specific points, I think you mentioned Eurodac. There is a distinction between Eurodac and the SIS proposals in the sense that Eurodac is a static system which is not updated on a real time basis and does not have in that sense the same direct operational impact at points of entry that SIS II would have. There is a distinction between the nature of the systems and how they operate. SIS II, when it goes live in the Member States, is a real time system that will be used as a basis on which to take immediate decisions in relation to persons at points of entry. I think there is that distinction which needs to be drawn between the two types of instrument. That said, you raise why management of SIS II by the Commission proved unpopular with Member States. If I am honest, that is in part as a result of a sense of a lack of trust between some Member States and the Commission, that lack of trust in part arising from the problems with the programme delivery at Commission level—in other words, with the technical difficulties, the programme management difficulties, that had arisen within the Commission's element of the programme and the extent to which those delays undermined Member States' confidence more generally in the Commission's ability to manage the system as a whole. From the UK's own perspective, I do not think we saw a particular difficulty in principle with the idea of the Commission managing the system but it is clear that a significant number of Member States, particularly some of the newer Member States, did find that they were unsure whether they could in that sense trust the Commission to deliver. That is why the notion of delegation of the management to a management authority with representation from all Member States is an idea that has been proposed.

Q37 ***Lord Avebury:*** Not merely proposed; we seem to be moving towards a decision that the cross-pillar agency will be responsible for the management. Could you say anything about the impact assessment that was mentioned as being a condition for the

creation of the cross-pillar agency? Has that been initiated or are there steps to programme it in?
Mr Sweet: My understanding is that it is factored into the process. There is a commitment and there will be an impact assessment produced in advance of the establishment of the management authority.

Q38 ***Lord Avebury:*** But you cannot say anything about the timescale?
Mr Sweet: Offhand, I am afraid I do not know the timetable but we can check on that for you. I am told it will be initiated once the instruments are formally adopted.

Q39 ***Lord Avebury:*** What is the timing on that?
Mr Sweet: I think it is expected that those might be adopted by the end of this year.

Q40 ***Lord Avebury:*** Can I ask you whether the government support the idea that other EU databases should be co-located with SIS II and, if so, which seems to be a suitable candidate? For example, would Eurodac be in the frame for co-location?
Mr Sweet: I do not think the government has any objection in principle to the idea of other EU database systems co-locating with SIS II. Co-location presumably in that sense means the physical proximity to those databases. There would clearly of course be resource implications if one were to move existing databases elsewhere. Our basic approach is if there were to be operational advantages and additional effectiveness as a result of co-location we would certainly support that in principle.

Q41 ***Chairman:*** Following on Lord Marlesford's earlier question, if other databases are being co-located and this led to us being excluded from those other databases, surely there would be very serious implications for us?
Mr Sweet: Yes. I was talking simply in the sense of physical, geographical proximity. You are absolutely right.

Q42 ***Viscount Ullswater:*** If I could move to the interim period, does the government believe that the provisions in the draft regulation concerning the accountability of the Member States which will manage SIS II for the transitional period—France, Strasbourg and Austria—are likely to prove adequate in practice? Could you say a little bit more about what you feel the right accountability should be for this Commission inspired agency, or is it a Member State inspired agency which might ultimately be managing the system?
Mr Sweet: My understanding is it is an agency which will have representation from all Member States and in that sense it is not a Commission body. That is part of the argument about the extent to which the Commission should manage the entire project.

Q43 ***Viscount Ullswater:*** Does that mean it will be a Commission funded body? Does it fall within the Treaty as being a Commission funded body or is it something like Europol? I do not think Europol is yet.
Mr Sweet: Europol is not yet.

Q44 ***Viscount Ullswater:*** Would it become like Europol?
Mr Sweet: I would have to check. I do not know the answer offhand.

Q45 ***Viscount Ullswater:*** I interrupted your train of thought on accountability.
Mr Sweet: Essentially we do think that there will be adequate provisions in place in relation to accountability for the management authority. The legal base specifically ensures that any delegation of the management of SIS II by the Commission does not adversely affect any effective control mechanism under Community law, be it by the Court of Justice, the Court of Auditors or the European Data Protection Supervisor. That is explicitly written into one of the Articles. In addition, the data protection aspects will be scrutinised by the European Data Protection Supervisor who must be given access to data and facilities as necessary to carry out his task. There are relevant provisions in the regulation and the Council decision providing for a review of the function of SIS II. Those relevant provisions include analysis of the output, cost effectiveness, security and quality of service. Reports on those, as I understand it, will be presented to the European Parliament and Council two years after SIS II becomes operational and thereafter every two years. We also expect that there will be further reports carried out by the Commission itself to evaluate the central system and the bilateral and multilateral exchange of information between Member States. Given that range of elements in it, we believe that the provisions in the regulation do provide appropriate accountability for the management of SIS II.

Q46 ***Lord Avebury:*** You mentioned the European Data Protection Supervisor who will have jurisdiction over the data protection aspects of the management of the project. Does that mean that you will have that duty on a day-to-day and ongoing basis and will you report in private to the management of the project or will these reports be available to Member States and the public?
Mr Sweet: I am not an expert on the data protection aspects, I fear, and it may be a question that might be better addressed to the Department for

Constitutional Affairs when they come along, as they in fact have responsibility specifically in relation to the data protection issues that arise in relation to this instrument.

Q47 ***Lord Marlesford:*** This is really a question about biometric data, so I think it must be for Mr Rejman-Greene. First of all, perhaps you could remind us exactly what biometric data it is proposed to incorporate in SIS II which is not in SIS I and what biometric data, if any, is in SIS I.
Mr Rejman-Greene: As far as I understand there is no biometric data in SIS I and, therefore, the introduction of biometric data in SIS II is a major step forward. My understanding is that there will be both face and fingerprint data stored in SIS II but the use of it will come in a staged process in accordance with the development of technology and the proving of that technology, first of all on the basis of use of fingerprints on a one-to-one basis—so is this a set of fingerprints which matched those which are asked for in SIS II—and that is obviously dependent on making sure that the technology is adequate. So there is a report that needs to be issued at that point, and at a later date the opportunity for a search of the entire database against those search requests as a set of fingerprints that the national Member State requires to match against what is in the database itself. There is a multi-stage process which depends upon the proving of the technology at each stage.

Q48 ***Lord Marlesford:*** That is face and fingerprints. I am surprised that you say the technology for fingerprint matching is not there yet. I thought—
Mr Rejman-Greene: It is certainly there and we certainly have, in the UK, experience of a very large database as well as other countries have. What we are talking about now is the rapid expansion of the database to many millions of records. We also have to bear in mind that each individual country will have their own standards and ways of enrolling people into a system and what needs to be checked is that that is being done across equivalent quality levels so that we do not get undue numbers of errors that would actually crop up which would then put a great burden on any fingerprint bureaux which would be checking that match process. So the technology is well developed; what is at issue is the implementation or use of that technology in this particular application.

Q49 ***Lord Marlesford:*** What is the timescale for this?
Mr Rejman-Greene: My understanding is that SIS II is expected to be brought in by 2009. There is a period of time (I believe it is two years) to allow the system to bed down and then the check on the technological capabilities has to be made to ensure that the system operates in a way in which a one-to-one match of a fingerprint or photograph operates correctly. At some time, which I believe is unspecified in the future, the search capabilities using identification will come into play.

Q50 ***Lord Marlesford:*** Just to recap then: first of all, the face and the fingerprints are going in tandem, but if the SIS II is coming in in 2009 they will not even start to use biometrics until 2011.
Mr Fitzpatrick: My Lord, may I interject at this point? Member States other than the UK will join SIS II in 2008 on the current timetable. Subject to the checks and so forth, we are expecting a properly developed programme covering all those checks to be put together by the Commission which contemplates implementation of biometrics in 2009, but it would obviously be subject to the assurance that the things that we have just talked about have been addressed to a certain extent. So that by the time the UK joins biometrics will be part of the system.

Q51 ***Lord Marlesford:*** Is it a problem of using them or of collecting them?
Mr Rejman-Greene: The problem is ensuring that the data is valid, accurate and usable. I believe there is a requirement within the process to ensure that that is correct for all users in order to ensure the validity of the results of the matching.
Lord Marlesford: The Information Commission itself has acknowledged that data protection in the UK is very complicated. I know that one of your colleagues said earlier that the Department for Constitutional Affairs was responsible for data protection but I think it would be very helpful if between the Home Office and that department you could give us a written note on exactly what the main points of conflict are between data protection and the collection and use of this data.

Q52 ***Lord Avebury:*** I wanted to pick up the point that was being made about the validity and usability of the data. Why does not the technology of Eurodac read across into SIS II? I appreciate there is not an interoperability treaty in this system but I would have thought that having developed a very large fingerprint database in Eurodac the lessons would have been learned and that it would not be so difficult as appears to be suggested to ensure that as far as fingerprints are concerned the new system of biometrics under SIS II will be robust.
Mr Rejman-Greene: I think certainly the lessons that have been gained through the use of Eurodac will certainly be implemented in the specification and development of this SIS II. My understanding is that Eurodac has a very specific role and a very specific set of requirements which have been developed in

redressing a very, very narrow field, which is, essentially, the asylum applications.

Q53 ***Lord Avebury:*** Yes, but, if I can interrupt you, that does not affect the methods of collecting and recording the data, does it? They have to be just as scrupulous about accuracy and validity of the records as a system which is collecting fingerprints for some other purpose.
Mr Rejman-Greene: At each level there will be a different level of competence required and what I understand from the Eurodac system (I am not an expert in Eurodac and if I am wrong I will certainly submit a written note) is that it is a simple return of "yes" or "no" to: "Is there anybody in the database with that set of fingerprints?" There is a large amount of extra information that is potentially available under SIS II. I think there the concerns are that there is a degree of a higher threshold of accuracy in a match and concern also in terms of the collection of data: first of all, the large number of countries and, also, the potential for error and the implications for criminals in the data protection context.

Q54 ***Viscount Ullswater:*** Before we move away from biometrics, is there any intention or do the regulations allow for the collection of other biometric data such as DNA? I am not thinking that DNA will be used for the point of entry but, obviously, it is an important one when dealing with criminal matters under pillar three which we might want to transfer from one European country to another.
Mr Rejman-Greene: I believe there is a provision there for an extension to other biometric modalities but at present there is no definite proposal on the table.

Q55 ***Earl of Listowel:*** What is the Government's view of the judgment in *Commission v Spain*? Is the Government content with the most recent text of the regulation as regards its application to family members of European Union citizens, considering that third-county national family members of UK nationals and residents could be affected by an SIS listing?
Mr Norris: The *Commission v Spain* (case 503-03) concerned the movement of, I think, Spanish nationals who had third-country national spouses—one family group living in Dublin in Ireland and the other living in London—who wanted to travel to Spain. Therefore, although they were travelling within the Community they were crossing the Schengen external border and there was a Schengen alert on the third-country nationals concerned. The Spanish Government considered that that in itself was a sufficient basis for refusing them entry into Spain—i.e. refusing them entry into the Schengen area. The Court of Justice said that essentially an alert entered into the Schengen Information System could not override the rights of free movement of EU citizens and their family members within the Community. Under the Free Movement of Persons Directive the movement of EU citizens and their family members within the Community can only be prevented on grounds of public policy, public security or public health, and there are a series of principles which have to be applied when taking any such decision. Essentially, the European Court of Justice said those principles had to be observed; it was not sufficient simply to refuse entry on the basis of an SIS alert alone. The text of the regulation has been amended since that judgment and we now have Article 15A, which specifically refers to the Free Movement of Persons Directive (Directive 2004/38), and I think we are now content with that article. The position under European Community law ought to be clear, both under the SIS II regulation and in the light of the European Court of Justice judgment.

Q56 ***Earl of Listowel:*** What compensation was offered to the family in question? Do you happen to know?
Mr Norris: I am afraid I do not have any information on that.

Q57 ***Chairman:*** Before I come to the last question, can I just revert to question two on your hymn sheet? I may have to ask you to repeat some points you made but I am not sure that I adequately covered the question. This is really the question of whether SIS I might be extended to the new Member States, but also the question of whether the technical limitations on SIS I would not actually make this quite difficult. Would it require a new regulation and a new decision? I think you may possibly have answered some of those questions but can we just do a rerun?
Mr Fitzpatrick: Certainly. I think I mentioned the issue. I think our view is that it would not require a new regulation because it would be perfectly possible to extend the system to the new Member States. However, from a UK perspective, we have not seen a proper impact assessment both from a technical perspective in terms of the capacity of the system and the capacity of the interconnections that would be required between Member States and the central system, and we have not seen a proper programme assessment of how long it would take, for instance, the recent so-called Portuguese SIS I for one4all It was suggested that if a decision was given on 16 October at a recent Council meeting to go ahead with that proposal it could be implemented (and there is a date by which it would be implemented) but there had been no proper assessment of the impact that pursuing that approach would have on SIS II, the timetable for SIS II and whether Member States

would be willing to commit the necessary resources to make it a reality.

Q58 ***Chairman:*** As of now it is likely that neither Bulgaria nor Romania will have any involvement in SIS when they become members at the beginning of next year?
Mr Fitzpatrick: That is true, yes, but that is also the same for other Member States who have recently joined.

Q59 ***Baroness Bonham-Carter of Yarnbury:*** On a point of clarification to Mr Norris, the alert that meant that these families could not go to Spain: was that purely because they were third-country nationals?
Mr Norris: No, it was an alert entered into the Schengen Information System flagging up that there are public security reasons for refusing the third-country nationals entry into the Schengen area, and that would apply to any third-country national trying to cross into the Schengen area.

Q60 ***Baroness Bonham-Carter of Yarnbury:*** So there was a specific reason.
Mr Norris: In this case, because the people concerned were not just third-country nationals but were family members of EU citizens with free movement rights, those additional free movement rights had to be respected.

Q61 ***Baroness Bonham-Carter of Yarnbury:*** They overrode the alert?
Mr Norris: Exactly.

Q62 ***Earl of Caithness:*** I would like to follow up my Lord Chairman's last question and your answer on that. Are you content for Her Majesty's Government to agree the proposals—I think you said on 16 October—when all the information that you have just alerted us to is missing?
Mr Fitzpatrick: No. The approval to start on 16 October would have been required at the JHA Council on 5 October and it was not given at that meeting. Several Member States, including ourselves, made representations that we were not yet ready and a decision was remitted until December to await further investigation and analysis, and we wait with interest to see what will be presented. However, of course, that is already a two-month delay to a purported delivery deadline of September 2007.

Q63 ***Lord Dubs:*** May I ask a question about the people going to Spain? If they had been coming from (this is a bit hypothetical) a non-EU country and heading for Britain in transit for a Schengen country would we have received an alert or does the alert system not work if people are in transit?
Mr Norris: We do not have access to the alerts issued which are entered into the Schengen Information System for immigration purposes, so we would not have had access to this alert.

Q64 ***Lord Dubs:*** I understand that the issue was not immigration as much as security matters.
Mr Norris: It was an immigration issue insofar as the Spanish Government were refusing them entry into Spain and therefore into the Schengen area. So it was the Spanish Government operating the immigration parts of the Schengen system and using these alerts which are entered into the system for the purpose of administering Schengen external border control provisions.

Q65 ***Lord Dubs:*** We do not get any of those?
Mr Norris: We do not have access to that data because we are not part of Schengen so far as the immigration side is concerned.
Lord Dubs: I thought it had security implications rather than immigration implications. Thank you.

Q66 ***Viscount Ullswater:*** So would Norway and Iceland, who are not members of the EU but *de facto* sort of members of Schengen, have had the alerts?
Mr Norris: They would because they are full members of Schengen even though they are not members of the EU.
Viscount Ullswater: It does seem to put us at a great disadvantage somehow. Ourselves and Ireland are the only two countries which are denied, for some reason which is quite difficult for me to understand, this information. I understand the reasons for it but I find it still difficult to agree with them, where other non-EU countries can share information which is certainly denied to us.

Q67 ***Chairman:*** Going back to earlier questions about financial contribution, I take it that Norway and Iceland make a financial contribution, do they?
Mr Norris: Yes.

Q68 ***Chairman:*** They do. Pro-rata?
Mr Norris: I am afraid I do not know what it is.

Q69 ***Lord Avebury:*** Is SIS II going to be discussed at the G6 Interior Ministers' meeting at Stratford on October 25, and the delays?
Mr Fitzpatrick: I am afraid I do not know the answer to that.

Q70 ***Lord Avebury:*** Is it on the agenda?
Mr Sweet: My understanding is that it is not on the agenda for that meeting, no.

Q71 ***Chairman:*** I think my last question follows on to Mr Norris. Given the evidence from the texts that we are going to be excluded from quite a lot in SIS II as we are from SIS I, is the Government considering legal proceedings against this?
Mr Norris: I think we are in a different position in relation to this regulation than we are in relation to European Border Agency regulation—passport regulation. As I explained earlier, in those cases we did purport to opt in and that opt in was not accepted and, therefore, we are challenging both of those regulations. I hope that the European Court of Justice judgment that comes out of those proceedings will sort out the principles on how far the UK can participate in these kinds of Schengen building measures. In this case, although we were not content with the position that UK asylum authorities are not to be allowed access to this Schengen information data on immigration data, I think the principles are different. It is not that we have been excluded from the regulation because it has been accepted that this was not a regulation that it would be appropriate for the UK to participate in; we did not send an opt-in letter. No arrangements have been made outside of the regulation specifically allowing UK asylum authorities access to this data for asylum purposes, and our approach is not to seek the annulment of the regulation but to pursue other means of getting access to this data, albeit in an indirect way. As we discussed previously, it does seem a bit odd if we are to be allowed access to the data why should we not be allowed direct access. Nevertheless, it looks as if that will be the position.

Q72 ***Chairman:*** Unless any of us has anything you want to add at this point, can I thank you very much indeed, all four of you, for appearing before us. I should, actually, have welcomed you back, Mr Sweet—and perhaps others—but certainly I apologise for not welcoming you back at the beginning.
Mr Sweet: Not at all.
Chairman: Thank you very much. That concludes the public session.

Supplementary written evidence by International Directorate, Home Office

Further to the House of Lords Select Committee hearing on Home Office evidence on the development of the Second Generation Schengen Information System (SIS II) the Home Office undertook to provide further information relating to a number of questions. The information is provided below, although we are awaiting information from the Spanish SIS programme team in response to question 56, which relates to the payment of compensation to the family in *Commission v Spain*. This information will be forwarded to the Committee as soon as it is available.

At Q6 the Committee enquired about the rescheduling document 12379/06, and the apparent secrecy surrounding this document. This document has been published and we have attached a copy at annex A to this letter.

Committee members asked for a list of the 80 authorities with access to SIS data. A list setting out the authorities that we intend to have access to SIS II is attached at annex B to this letter for your information, but we would request that you do not publish this as it is restricted information. It is possible that the precise list will change between now and the connection of the UK to SIS II.

At Q17 the Committee asked about the added value of SIS I, to which Mr Fitzpatrick replied that there was some very useful information from other member States about the number of alerts and the number of arrests that they are able to make through SIS I. This data was published in Council document 5913/06 and is attached at annex C to this letter. This document is restricted and we therefore ask that you do not publish it.

At Q31 the chairman requested any further information the Home Office holds on the formula by which the UK pays a full subscription to the costs of the SIS II but does not have full access to the information. We do not participate in the Schengen immigration and border control rules, and we will not therefore have access to the data entered for border control purposes. We pay a full subscription, however, as set-up and running costs are determined by the infrastructure needed for the system itself, rather than the data held in it.

In addition, we maintain that we should have access for law enforcement and asylum purposes to entry refusal alerts on third country nationals, if other Member States are using the data for such purposes, and will continue to seek such access to alerts on persons refused entry on the grounds they represent a serious threat to public security or national security. The fact that we pay a full subscription supports this argument.

11 October 2006

At Q38 the Committee asked about the timescale for the setting up of the management authority and the impact assessment which would need to be produced in advance of the establishment of this authority. A proposed joint declaration of the Commission, the Council and the European Parliament on Article 12, relating to operational management, sets out these timescales. This draft declaration is appended to documents 5709/10/06 and 5710/7/06, which were deposited for scrutiny on 25 October. In this the Commission commits itself to presenting the necessary legislative proposals needed to set up the management authority within two years of the entry into force of the Regulation. The European Parliament and the Council also commit themselves to dealing with these proposals as quickly as possible, and to have them adopted in time to allow the agency to take up fully its activities before the end of a five year period following the entry into force of the Regulation.

The Committee also enquired about the nature and funding of the management authority at Q44. As set out in Article 12, the agency will be funded by the budget of the European Union. It shall be responsible for the operational management of the Central SIS II, as well as the following tasks related to the Communication Infrastructure: supervision; security; and the coordination of relations between the Member States and the provider. It will be funded from the Community budget.

The Committee was particularly interested in the inclusion of biometric data in the information held in the SIS II, and asked a number of questions relating to this subject. Further to this exchange we are providing the Committee with some additional explanatory information on the use of biometrics in the SIS II.

Photographs will only be used for verification purposes, ie to confirm the identity of a person after an alphanumeric check has identified them. Fingerprints will likewise only be used for verification purposes initially, and their use for any purpose beyond simple verification of an individual's identity will not be introduced until the Commission has presented a report on the availability and readiness of the technology, ie when the Commission is satisfied that the real capabilities of biometrics for identification purposes are sufficiently advanced. Member States will then have to be satisfied with this report and the opinion of the European Parliament will be sought.

Once the technology is sufficiently advanced, fingerprints will be used for verification in certain circumstances. There is a distinction between verifying someone's identity, which is proposed, and trawling the fingerprints database in order to identify a fingerprint from a crime scene, which we do not anticipate doing at this stage, or in any routine manner in future.

Furthermore it is important to note that biometric searches can be used in order to minimise the misidentification of persons, by providing an additional means to facilitate correct identification. The use of fingerprints and photographs should reduce the incidences of misidentification: people with the same name are fairly common but use of fingerprints will easily confirm whether or not a person whose name is in the SIS II is indeed the subject of the alert.

At Q68 the committee enquired about the financial contributions made by Norway and Iceland. The total costs for the maintenance and running of the SIS infrastructure is published but there is not a country-by-country breakdown provided. The EU Member States pay a share of the cost according to the percentage GDP/capita of the EU they constitute. The UK contribution is typically between 18 per cent and 20 per cent. As Norway and Iceland are members of the European Economic Area but not members of the EU this formula does not apply to them, although they do contribute to the costs.

The Committee also asked whether SIS II was due to be discussed at the G6 meeting held in Stratford-upon-Avon in October 2006. Although not a formal agenda item in its own right, and not discussed in any depth, Ministers did reaffirm their commitment to the rapid conclusion of negotiations on the SIS II, during discussions on tackling organised crime.

The Committee may also wish to note that, since this evidence session, the European Parliament voted to adopt the legal instruments at First Reading on 25 October, without the late amendment to Article 37 of the Council Decision. We expect the Council to accept the texts as adopted by the EP.

1 November 2006

11 October 2006

Memorandum by the Meijers Committee[1]

1. Introduction

On behalf of the Standing Committee, we would like to submit some general comments on the development of the second generation Schengen Information System or SIS II. In these comments we will focus on the draft Regulation on SIS II, based on the revised text as agreed upon during the meeting of the EU Ministers of Justice and Home Affairs of 2 June 2006.[2] It should however be underlined that the adoption of this Regulation is to be considered in close connection with other developments in the EU. Firstly, the future use and impact of SIS II will be determined by the final texts of the Decision on SIS II for policing purposes (COM (2005) 230) and the Regulation giving access to SIS II by vehicle registration authorities (COM (2005) 237). Secondly, which authorities will have access to SIS II and the further use of this information will depend on the final decision-making with regard to the proposed Visa Information System (VIS), the future use of Eurodac, and the inclusion of biometrics in the EU databases and the EU passport. The fact that different drafts of these proposals are still circulating, makes it difficult if not impossible to assess the full implications of the future developments at this moment. Thirdly, it is important to be aware that national developments are decisive for the future use of SIS II. Important factors are of course the national criteria on the basis of which data are entered into SIS II and the accuracy and reliability of these data. But it should also be taken into account that the introduction of new technologies for surveillance purposes at the national level, including biometrical identifiers, facial recognition systems, or automated license plate readers for vehicles, could extend the use and availability of SIS II information beyond its anticipated goals.

In the following paragraphs we will deal with the following aspects of the draft Regulation on SIS II:

- Decision-making process.
- Operational management—accountability.
- Inclusion of biometrics.
- Clarity of rules governing collection of and access to data.
  - (a) Criteria of third country nationals to be stored into SIS II.
  - (b) Authorities receiving access to SIS II.
- Adequacy of data protection rules—rights of individuals
  - (a) Applicable rules.
  - (b) Purpose Limitation.
  - (c) Individual rights and legal remedies.

2. Decision-making Process

The Standing Committee is concerned about the lack of transparency with which the proposals on SIS II are currently adopted. The Standing Committee emphasises that the development of SIS II is an extremely important subject which includes the set up of a very large database, involving the registration of millions of individuals, including family member of EU citizens. This database will have a large impact on the movement of individuals, not only because of the proposed use of biometrics, but also because of the implementation of the principle of interoperability, as proposed by the European Commission (COM (2005) 597). Although the Commission has not yet submitted more specific proposals, the principle of interoperability refers not only to the common use of large scale IT systems (SIS II, Eurodac, VIS), but also to the possibility of accessing and exchanging data or even merging the different databases. The establishment of SIS II and its shared use with other EU databases require careful scrutiny by the European Parliament and national parliaments. Their involvement has been made difficult by the piecemeal approach with regard to decision-making on SIS II and the other databases. Between 2001 and 2006, different legislative measures, including decisions on the technical features of SIS, have been adopted by the Council. These decisions gradually allowed for an extended use of SIS. Further it should be noted that the original proposals of the Commission differ from the most recent drafts and that these latter texts have been made accessible neither to the general public nor to the national parliaments.

[1] Standing committee of experts on international immigration, refugee and criminal law.

[2] For our comments we have used the text as adopted on 6 June 2006, doc 5709/6/06, see the website of Statewatch: www.statewatch.org

The co-decision role of the European Parliament with regard to the draft Regulation on SIS II has to be welcomed, as well as the improvements of the final text as proposed by the European Parliament. However, the confidential negotiations between European Parliament, Council, and the European Commission, do not provide any insight why on and on whose behalf final decisions or compromises have been reached. It is still unclear whether the text which has been agreed upon by the EU Ministers of Justice and Home Affairs in their meeting of 2 June 2006, must be considered as the final compromise text between European Parliament, Council, and Commission, or whether this text will receive full scrutiny by the European Parliament, when dealing with it during its plenary sessions. In this regard, the Standing Committee refers to the adoption of the Regulation on the Community Borders Code in 2005.[3] Based on the concerns of the Council and the European Parliament to have this legislative proposal adopted during the first reading of the applicable the co-decision procedure, the compromise text as agreed upon during the tripartite negotiations was considered as the final version even before the public plenary session of the European Parliament. In the view of the Standing Committee, this chosen procedure of decision-making hampers the transparency of legislative procedures within the EU.

3. Operational Management—Accountability

In a note of 15 May 2006 on the issue of long-term management of SIS II, the Austrian Presidency proposed to set up a special Agency for the management of SIS II, and possibly also for Eurodac and VIS.[4] In the text of the draft Regulation on SIS II as agreed upon on 6 June 2006, this proposal has been included in a new Article 12 dealing with the tasks and responsibilities of a "Management Authority". This Management Authority should after a transitional period perform the tasks of the Commission with regard to the supervision, security, and coordination of relations between Member States and the provider of SIS II. The Standing Committee is in general concerned about the institutional consequences of the set up of new agencies in the legal framework of the EU. The setting up of a separate agency or Management Authority might have its practical and budgetary benefits, but it should be prevented that such authorities receive EU responsibilities and competences and at the same time will be able to operate quite autonomously from the EU institutions. In the view of the Standing Committee, the setting up and the functioning of such agencies, including the Management Authority, should be made dependent on the following guarantees:

- full competence of the European Court of Justice to assess the lawfulness of the activities and decisions of these agencies or authorities;
- clear rules on their liability;
- clear and coherent rules with regard to the responsibility of the European Commission; and
- application of the general EU rules on access to documents of the EU institutions.

4. Inclusion of Biometrics

Article 14 C of the draft Regulation as agreed upon in June 2006, includes the option that biometric data to be entered into SIS II will be used as identifier. Or with other words, SIS II will be searchable on the sole basis of biometric data such as photographs or fingerprints without needing additional data on the person concerned such as name and surname. This use of biometrics as an identifier has been explicitly rejected by the European Commission, but also by the European Data Protection Supervisor and the Article 29 Working Group, on the basis of the fact that the technological reliability does not allow for a secure and reliable identification. Using biometrics as sole identification key still entails a too high risk of false identification or false non-identification (compare: "false rejection rate" and "false acceptation rate"). Even if only one or a half per cent of the persons would be wrongly identified on the basis of biometrical data in SIS II or VIS, considering the millions of person to be recorded in these databases, still the number of persons affected by automatic negative decisions will be much too high. Different organisations warned that the use and central storage of biometrics will extend the risk of unauthorised access to these databases, the misuse or manipulation of biometrical data by criminal organisations, and the possible increase of identity theft. These negative aspects, as well as the impact of the use of biometrics for the privacy and human rights of individuals, have not been appropriately taken into account in the decision-making process.

[3] Regulation 562/2006 of 15 March 2006, OJ L 105/1, 13.4.2006.

[4] Council doc 9169/06.

5. Clarity of Rules Governing Collection of and Access to Data

(a) *Criteria for third country nationals to be stored into SIS II*

The adoption of the Regulation on SIS II would have been an excellent chance to harmonise the applicable criteria for the registration of third country nationals to be refused entry. The original proposal of the European Commission of May 2005 included a useful proposal for such harmonisation. It is regrettable that Article 15 of the draft as agreed upon by the Council in June 2006 returns more or less to the same criteria as included in the actual provision of Article 96 of the Schengen Convention (SC). The actual use of Schengen Information System (SIS) has shown that the implementation of these criteria varies considerably between the Member States using SIS. The difficulties which arise from such differences in interpretation can be illustrated by the annual reports of national data protection authorities and judgments of national courts dealing with decisions based on foreign SIS alerts. It is to be feared that the extended use of SIS II from 15 European states to more then 25 states, will only increase the problems caused by the different interpretations of the criteria as provided in Article 15.

The criteria in Article 15 (2) of the draft Regulation of June 2006, include two important extensions of the applicable criteria compared to the original text of Article 96 SC. Firstly, Article 96 (2) (b) SC requires that a decision to report a person into SIS should be based on "serious grounds for believing that he has committed serious criminal offences or in respect of whom there is clear evidence of an intention to commit such offences in the territory of a contracting party." Based on the proposed Article 15 (2) (b), "clear indications of an intention to commit such offences" are considered sufficient for registration into SIS II.

Secondly, the proposed Article 15 AA provides that third country nationals may be registered into SIS II on the basis of a decision taken in accordance with Article 15 of the EU Treaty. This new category refers to persons listed in the EU terrorist lists based on the travel ban as issued by the Security Council of the United Nations. The Standing Committee is in general concerned about the secret and unclear criteria on the basis of which third country nationals are listed as "terrorists". The automatic inclusion of these persons into SIS on the basis of which they will be refused entry should be accompanied by minimum guarantees preventing erroneous registration in SIS II. The concerns of the Standing Committee are strengthened by the fact that Article 15 AA (2) includes an exception to the general rule of Article 14 D, that an alert cannot be entered without the information on the name, sex, a reference to the decision giving rise to the alert, and the action to be taken. It is unclear how persons listed in the EU or UN terrorist list can be registered in SIS II without their names or referring to the action to be taken, unless it is the intention of Member States to enter these persons into SIS II solely on the basis of the use of their biometrical data such as fingerprints.

It is to be welcomed that, as proposed by the Commission, the final text of the Regulation includes the obligation for Member States to erase alerts on persons as soon as the Member State which issued the alert becomes aware that the person acquired EU citizenship (Article 20 AA). The Standing Committee regrets however that the final text does not include the obligation, as proposed by the Commission, to erase data on third country nationals who become family of EU citizens as well. This omission seems to be in contradiction with the judgment of 31 January 2006 of the ECJ in the case Commission v Spain (C-503/03). In this judgment, the ECJ ruled that the listing of third country national family members of EU citizens in SIS, and more specifically the automatic decision-making on the basis of this listing, infringes the rights of these persons under EC law.

(b) *Authorities receiving access to SIS II*

In the original proposal of the Commission of May 2005, information on third country nationals stored in SIS would only be accessible for authorities responsible for border controls and for authorities issuing visas. Article 17 of the draft Regulation of 6 June 2006 provides that access to information stored into SIS II in accordance with Article 15 will be reserved exclusively to authorities responsible for border control and for "other police and customs checks carried out within the country, and the coordination of such checks by designated authorities". Although the Standing Commission welcomes the addition of the words "exclusively" and "designated authorities", it should be noted that "authorities responsible for police checks within the country" still includes an extremely wide category of officials. This implies the use of SIS II and the information on third country nationals therein for other purposes than only border control or visa applications. Although Article 17 A of the Regulation on SIS II provides that users "may only search data which they require for the performance of their task", it is questionable whether the general provision will prevent police officers from starting general searches in SIS II when checking persons within the national territory for public order reasons.

Article 34 (2a) of the Regulation on SIS II includes the obligation for the Management Authority to publish each year statistics showing the number of records per category of alert, the number of hits per category of alert and how many times the SIS II was accessed. It might have been useful if these statistics also included other information, for example on the authorities which actually obtained access to SIS II, the nationalities of persons stored into SIS II, or on the decisions or measures which have been taken on the basis of SIS II information. This would make it possible to assess the added value of SIS II more completely.

6. Adequacy of Data Protection Rules—Rights of Individuals

(a) *Applicable rules*

The data protection regime applicable to SIS II and other EU databases is complicated by the two pillar dichotomy which accompanies the current legislation. On the one hand, data processing through SIS II falls within the scope of the Data Protection Convention of 1981 of the Council of Europe and, if adopted, the EU framework decision on third pillar data protection. On the other hand, the processing of data on third country nationals to be refused entry as provided in the Regulation on SIS II falls within the scope of the EC Directive 95/46. This latter Directive will also apply to the proposed VIS, except for the proposed dissemination of VIS data to internal security authorities and to Europol (COM (2005) 600): this would fall under the third pillar data protection rules.

In view of transparency and equality, the simultaneous application of different sets of rules with regard to the processing of the same personal information is undesirable. Not only individuals, but also the authorities using these systems need to know which rules apply. The ratification of the Constitutional Treaty of the EU by all Member States would have solved this problem partly because of the proposed collapsing of the three pillars, which could have been an extra motive to extend the application of the EC Directive 95/46 to the general field of EU law. As long as the three pillar construction applies, other solutions will have to be found to solve the problem of divergent data protection rules. One solution could be to adopt on a very short term the proposal for a framework decision on data protection in the third pillar.[5] However, this option should be made dependent on the following requirements:

- Inclusion of a high level of data protection standards in this framework decision.
- The framework decision should be applied as specification and not limitation of the general data protection principles as included in the EC Directive 95/46 and Article 9 of the EU Charter of Fundamental Rights. This has been explicitly underlined by the Commission in its explanatory memorandum to the proposal of the framework decision.
- The scope of the framework decision should be extended to the use of personal data by Europol and Eurojust and other authorities or agencies using personal information for law enforcement, judicial, or internal security purposes. Aside from the transmission of data between member states, the framework decision should also cover data processing within the member states. It should prevent data processing which falls within the scope of EU law, from falling outside the scope of EU rules of data protection and, thus, may fall outside the scope of any rule of data protection.
- The individual rights to information and to access, correction, and deletion of data, as well as the right to legal remedies should be in conformity with the applicable rules in the other instruments of data protection. It would be unacceptable if the level of data protection for an individual with regard to the same information in the same database, would be made dependent on the authority having access to this data or the purpose for which this has been transmitted to other authorities.

(b) *Purpose Limitation*

The purpose limitation principle is one of the key principles of data protection. It safeguards the transparency and legality of the use of personal data. The Standing Committee is most concerned about the fact that this fundamental principle is rendered meaningless by current developments. These developments include in the first place the vague and open definitions of the goals for which new EU databases are set up. For example, the purpose of SIS is described in the SIS II Regulation proposal as: "to maintain public policy and a high level of public security, including national security in the territories of the Member States and to apply the provisions of Title IV of the Treaty establishing the European Community relating to the movement of persons in their territories, using information communicated via this system". The goal of VIS has been

[5] COM (2005) 475.

presented from the beginning as a "multifunctional tool". VIS will not only be used for the implementation of EU visa policy, but also for the fight against illegal immigration and terrorism, and to return illegal immigrants. As we have seen above, a draft has been prepared to give national internal security authorities and Europol access to VIS as well. Secondly, recent proposals of the Commission on interoperability of databases (COM (2005) 597) and the principle of availability (COM (2005) 490) are in absolute contradiction with the principle of purpose limitation. National and European data protection authorities repeatedly underlined the importance of purpose limitation and have warned against the risk of "function creep". Allowing the use of personal information, including biometrics, by different authorities for different purposes not only entails the risk of wide dissemination of unreliable information, but will also threaten to infringe the rights of individuals concerned.

(c) *Individual rights and legal remedies*

The refusal of entry based on SIS II, the wrongful identification based on biometrics stored in SIS II or VIS, or the unlawful transmission of personal data to third parties or third countries, all include the risk of violating fundamental rights as recognised in the European Convention on Human Rights and the EU Charter of Fundamental Rights. Both the European Court of Justice and the European Court of Human Rights have repeatedly underlined the importance of the right to privacy and data protection, formulating stringent criteria for measures interfering with these rights.[6] At the national level, the German Constitutional Court recently ruled that large scale data searching ("Rasterfahndung"), a measure which has been used by the police in Germany to trace terrorists by gathering information from different databases, constituted a disproportionate infringement of the individual's right to privacy.[7] Refusals of entry based on SIS information further risk of violating the Community law rights of third-country nationals to enter and reside in a Member State, granted by Directive 2003/86/EC on the right to family reunification or Directive 2003/109/EC on the state of long-term resident third-country nationals. In its judgment of 27 June 2006 in the case *EP v Council* (C-540/03) the Court affirmed that the first Directive grants a subjective right to family reunification to spouses and minor children without a margin of appreciation being left to Member States (paragraph 60 of the judgment).

Considering the developments described above, the legal protection of individuals is an absolute requirement. Individuals should have the right to accessible and effective remedies with regard to the use of SIS II. The actual practice of SIS shows that a huge problem for individuals is the fact that they often do not know that they are recorded into SIS for the purpose of refusal of entry. They will only discover this when applying for a visa or when being checked at the borders. The Standing Committee regrets that the original proposal of the European Commission to oblige national authorities to inform a person in advance on the processing of his or her data in SIS II (including identity of controller, purposes, potential recipients) has been deleted. The new draft only includes the (general) right of the individual to apply for access, rectification, or correction.

The removal of the territorial limitation included in the original Commission proposal is important with regard to the access to legal remedies. Article 30 (1) of the draft of 6 June 2006 now provides that any person may bring an action before the courts or the authority "in particular to correct, delete or obtain information or to obtain compensation in connection with an alert involving them". This means that, unlike the original proposal, access to remedies is no longer dependent on whether the person actually is within the territory one of the EU Member States. Especially where it concerns the use of SIS II for the refusal of entry or a visa, it would have been unacceptable if a third country national would not be able to remedy the wrongful use or registration of his or her personal information if he or she would be outside the EU territory. The Standing Committee recommends that this territorial limitation will also be lifted in the other proposals on SIS II or VIS.

Further, the text of the Regulation on SIS II re-introduces in Article 30 (2) the obligation for national authorities to enforce mutually the final national decisions of courts or authorities as set out in Article 30 (1). This provision which already has been included in Article 111 (2) SC, is a very important safeguard for individuals. This provision ensures that decisions taken by independent authorities on the lawfulness of a national alert in SIS will have to be enforced in other Member States as well. The actual practice of SIS shows however that national authorities often are reluctant to enforce the decisions of foreign courts or data protection authorities. The re-inclusion in the Regulation on SIS II could be a new impetus to enforce this mutual recognition. Another problem is caused by the fact that national courts do not always find themselves competent to assess the lawfulness of a foreign decision when dealing with a third country national whose

[6] ECJ: C-101/01 *Lindqvist* OJ C7/1, 10.01.2004 and C-456/00 *Österreichischer Rundfunk* in OJ C171/3, 19.07.03; ECtHR: *Rotaru*, 4 May 2000, appl no 28341/95.

[7] BVerfG, 1 BvR 518/02, 4 April 2006.

entry or visa has been refused on the basis of a SIS alert. This problem is also due to the lack of harmonised criteria for entering persons into SIS II. One of the solutions to this problem could be to extend the competence of national courts to forward preliminary proceedings to the ECJ. This could enable the Court to clarify the applicable criteria and to assess the necessity and proportionality of the measures involved.

Finally, in Article 30 (3) of the Regulation on SIS II, it is provided that the Commission will evaluate the rules on remedies provided in this Article, two years after the Regulation enters into force. This evaluation will be an important tool to assess both the accessibility and effectiveness of the remedies in the different Member States.

10 July 2006

Memorandum by the Immigration Law Practitioners Association (ILPA)

1. This association, which is comprised of immigration practitioners primarily in the UK, shares the view of the Committee of the House of Lords that the development of the SIS II system merits investigation in detail. We are, therefore, both honoured to participate in this inquiry and very interested in the subsequent report.

2. We have had the pleasure of reading the evidence submitted by the Standing Committee of experts in international immigration, refugee and criminal law with which we are in broad agreement. Accordingly, we will not repeat comments and issues which have already been taken up in that memorandum to your Lordships, except and unless our view differs from that the expressed in their memorandum.

Decision Making Process

3. As the original SIS was developed in fairly comprehensive secrecy among the five original Member States of the Schengen Agreement (though subsequent adherent states were involved), the degree of availability of information regarding the development of SIS II is refreshing. Nonetheless, shortcomings are still evident. What is particularly evident in the documents which have been published by the Commission and those available on the Council's website under the transparency arrangements is that SIS II is consistently presented as a technical matter. The language employed is full of technical phrases, concerns about capacity and the like. Indeed, even the need for a new generation SIS was presented on the grounds of enlargement of the EU and the additional demands which ten new participants would make on the system. More important, in our view, than the technical issues of the SIS II, are the new capacities which it appears the SIS II will have and their consistency with fundamental rights of individuals. As many of the newer Member States are still painfully aware, the collection, retention, manipulation and use of data about the individual by the state has been critical to the maintenance of power by totalitarian regimes. One of the first things which occurred in the post 1989 period in Central and Eastern Europe was the massive destruction of files on individuals held by the Securitate and their ilk. It would be unwise to underestimate the importance of the right to privacy to democracy in Europe. While transparency must be the guiding principle in the activities of the state, the right to privacy is paramount for the individual. Coercive practices in some parts of Europe have been built on the inversion of these relationships.

Operational Management

4. Our key concern regarding management of the SIS II system is not so much which institution is responsible but rather what rules apply. It seems to us that it is unclear how the right of privacy of the individual is being protected in the EU at the moment. While the principle is contained in the European Convention on Human Rights (article 8 which prohibits state interference unless justified on limited grounds) and in the EU's own Charter of Fundamental Rights, there is no clarity on how the right is protected. What is clear is that unlike the US system, nowhere in the EU in the protection of his or her privacy (and data) considered a matter exclusively for the individual and for him or her to pursue single-handedly in the civil courts. In all Member States, as far as we are aware, there are institutions established by statute and paid out of public funds, whose job it is to protect the individual's data. While this may be in the form of ombudsmen with direct responsibility, or of national agencies with indirect access, nonetheless the principle is the same. The state accepts a substantial degree of responsibility to protect the individual against the state in this field.

5. The question which arises in the case of SIS II is how is the individual's data protected when the entity collecting, storing, manipulating and transmitting the data is not the state or a private actor within the state's control, but a supranational actor in whom the state participates. Can the state systems of protection adequately protect the individual or are other entities and systems required? The highly active role which the

European Ombudsman has taken to ensure transparency of EU policy making might be an example for the European Data Protection Supervisor as regards the protection of personal data. But the remit of both these EU institutions may be too limited to provide the effective control which fundamental rights norms require.

6. There is also a political question which arises here—if the citizen of the Union (particularly some of the citizens in the newer Member States) is vitally concerned about the collection and use of data on him or her (to the extent of burning the files less than 20 years ago), should national institutions be responsible for protecting the citizen against the supranational authority peeping into his or her life? Or should the EU institutions protect the individual's privacy, including from the national authorities excessive curiosity?

Biometric Data

7. There is much concern at the moment about the collection, retention and use of biometric data. In our view this is fuelled by the presentation of biometric data as a solution to the certainty of identification of individuals. While it is certainly the case that biometric data used in certain controlled situations can give fairly accurate indications of the identity of an individual, the parameters around that identification must be borne in mind. There is nothing automatic about biometrics—an official is required at all times to ensure that the biometric information being fed into the system corresponds to the individual who is feeding it in. Thus the impression of automaticity in the use of biometrics is not entirely accurate. For instance if a numeric photo is held to a camera and the image corresponds to the numeric photo which the computer at the other end of the numeric camera is expecting to receive, there is a full correlation; but this does not say anything about the person holding the numeric photo. The use of biometric data only moves one step on the point of verification that the biometric data actually belongs to the individual presenting it. However, the collection, storage, use and transmission of biometric data on some grounds, of individuals within a community, to the exclusion of other groups, places the monitored group substantially further under the control of the state's coercive forces than others as we explain in the next paragraph.

8. For instance, if the EURODAC data base were made available to law enforcement agencies in the Member States, asylum seekers who committed crimes would be discovered almost to a man. Thus the clear up rate of offences committed by asylum seekers would, statistically speaking, be excellent but would indicate a highly level of criminality among asylum seekers than among the domestic population. This impression would, of course probably be wrong, as the statistics would be based on the access to finger print data on all asylum seekers and the sparse fingerprint data available on nationals of the state. But the public imagination could easily be manipulated against asylum seekers on the erroneous conclusion that they are more prone to criminality than the domestic population.

9. DNA data presents even further problems. We understand that this type of biometric data can provide information on sex and race. Such data is inherently dangerous as the European experience in 1940–45 has shown.

Interlinking Alerts

10. The problem here is one of the transfer of data. Even where an authority has justified the collection and storage, for a limited time, of personal data, it cannot be presumed that the transmission of that data to another authority, even within the state, is justified. The principle of privacy in European human rights law mitigates against any such assumption. Transmission of data is among the most sensitive of issues regarding the right of the individual to privacy. While the individual may agree to the collection and retention of his or her data for one purpose, he or she may be vehemently opposed to its transmission to another authority—for instance information provided to state health services being transmitted to government agencies engaged in insurance or taxation. Alerts are only another way of speaking of personal data about individuals. While the legitimate interest of the state to find persons suspected of criminal offences may justify the release of data, it is inconsistent with the right of the individual for this to happen on the basis of automaticity.

Criteria for Listing Persons to be Refused Entry on the SIS

11. One of the key legitimacy issues of the SIS has been that the vast majority of the data on individuals held on the system is data about third country nationals to be refused admission to the EU. Thus the SIS has become a glorified immigration database rather than a tool in law enforcement in criminal matters (outside immigration offences). While the grounds for inserting law enforcement data on the SIS has been fairly well defined, the criteria for the inclusion of data concerning third country nationals has been woefully vague. A

number of cases have come before the national courts of the EU on this question and the solutions have been diverse. What is particularly interesting is that the EU (whether in the form of the Commission, or the Council of Member States) has not taken this occasion to clarify and simply the rules on whose data should be included and whose removed. We understand that even two years on from the last enlargement of the EU some "old" Member States are still trying to clear out their alerts on nationals of "new" Member States—which alerts are not justified on the grounds of public policy, security or health as required by EU law. The decision by the European Court of Justice in the Commission's action against Spain for including data in the SIS on family members of Union citizens is particularly instructive of how the issue of the inclusion of data on the SIS might be tackled. The Court held that while data on third country national family members of Union citizens could be held on the SIS, the reason for their inclusion must comply with EU law. Specifically they need to be a serious risk to public policy, security or health as interpreted by the Court in previous rulings. One might consider this ruling to be a type of "taming" of the SIS in that the lawfulness of the inclusion of data will be controlled by the rules of EU law not the vague rules which are contained in article 96 CISA. Whether this optimistic reading of the ruling will prevail is still to be seen.

Use of Data

12. As we have set out above, one of the most important and legitimate concerns of the individual as regards the collection and retention of his or her data is whether it remains within the control and exclusive use of the agency which has collected it, or whether it acquires a life of its own, passing willy-nilly through different databases and different agencies around the EU or indeed the world.

The current controversy over the agreement between the Belgian operators of the SWIFT banking transfer system with the CIA exemplifies exactly this problem. Individuals transferring funds around Europe through the SWIFT system were happy to provide their data to their banks but are aghast at the prospect that that data was subsequently passed on to the CIA without their knowledge or consent. The European understanding of the right of privacy mitigates against any further transmission of data unless under very specific and precisely argued rules.

Adequacy of Data Protection

13. There has been a tendency over the past few years on the part of some state authorities to seek to interpret the fundamental right of privacy as consistent with rather relaxed practices of data exchanges and use among state institutions. This period appears to be coming to an end. The German Constitutional Court has had the occasion to consider and reject the manipulation of data for the purposes of racial profiling. The European Court of Human Rights has recently handed down a judgment reinforcing the right of the individual to protection of his or her data from interference by state authorities. The EC Data Protection Directive provides fairly clear rules (though insufficient, it would seem from the judgment of the European Court of Justice in the PNR case) to protect individual data. The EU's second and third pillars lack data protection measures and the framework decision proposed by the Commission for data protection in the third pillar is weaker as regards the protection of the individual than that already adopted in the first pillar. The collapsing of the pillar as proposed by the draft constitutional treaty would have resolved this issue, bringing a consolidated regime into existence with the data protection directive applying across the board (or almost and subject to its weakness as identified in the PNR judgment). The Commission has recently proposed the use of article 42 TEU to bring the third pillar into the first, which presumably would have the effect of bringing third pillar activities under the control of the data protection directive. This would be most welcome. The strengthening of the data protection directive would also be valuable bearing in mind the recent judgments in Karlsruhe and Strasbourg.

Finally, the UK's position: anomalous as it is, there is little which can be added other than to note that where a state does not participate in a treaty because it is unwilling to accept the freedom required by it, it cannot reasonably expect to enjoy the coercive benefits of the treaty.

13 July 2006

WEDNESDAY 18 OCTOBER 2006

Present	Avebury, L	Dubs, L
	Bonham-Carter of Yarnbury, B	Henig, B
	Caithness, E	Listowel, E
	Corbett of Castle Vale, L	Wright of Richmond, L (Chairman)

Examination of Witnesses

Witnesses: PROFESSOR KEES GROENENDIJK, MS EVELIEN BROUWER and PROFESSOR THEO DE ROOS, the Meijers Committee (the Standing Committee of Experts on International Immigration, Refugee and Criminal Law), and PROFESSOR ELSPETH GUILD, ILPA (Immigration Law Practitioners' Association), examined.

Q73 ***Chairman:*** Good morning, ladies and gentleman, to be joined by another gentleman shortly; I understand that he is on his way. Welcome to all of you. If I may say, Ms Brouwer, a special welcome to Professor Groenendijk and to Elspeth Guild who are longstanding friends of this Committee, or at least I hope you regard yourselves in that way. This session is on the record and you will in due course be sent a transcript of the evidence for you to check that we have it correctly recorded. It is being broadcast but not televised. It is very good of you to come and particularly good of you to come from some way away. Do any of you want to make any opening statement or opening comment?

Professor Groenendijk: First of all, I would like to thank you for the invitation and once again commend this subcommittee for its very important contribution to democracy and rule of law in Europe by holding these kinds of hearings. It is the only national parliament which does so. I think that the issue of SIS is especially important because the questions you have formulated and the issues you are discussing now arise in regard to the Schengen Information System that contains personal data of about 700,000 to 800,000 third country nationals but the same questions will arise or are on the table with regard to the Visa Information System which will contain the data on millions of third country nationals. So, the theme is a very important one. If you will allow me to draw one more parallel, I remember that, during the negotiations on the Schengen Implementing Agreement in 1989, there was a great deal of pressure put on discussions around issues such as remedies and protection of privacy, but then we had to rush because everything had to be agreed in 1990 in order that the system could be in place in 1992. Eventually SIS became operative only in 1995. Now, we have exactly the same pressure again, that everything should be decided within a few months and even now there is talk about SIS II being operative in 2008. Why do we not take some time to discuss these very important issues and why do we allow ourselves to be rushed—and I will not say by the politicians because that may be a bad thing to say in this House?

Q74 ***Chairman:*** Thank you very much for that. Incidentally, I should have thanked Elspeth Guild and Ms Brouwer for your written evidence.

Professor Groenendijk: May I introduce Ms Brouwer? She is a PhD student at the Radboud University Nijmegen. She is writing her dissertation on the functioning of the Schengen Information System in France, Germany and the Netherlands. That is why we are very happy to have her on our Committee. Professor de Roos will arrive at any moment; he is on another plane.

Q75 ***Chairman:*** When it is written, I hope that you will send us a copy. I think that my first question leads on very much from what Professor Groenendijk has said because it is a rather speculative question and that is, what improvements could have been made to the process of negotiating the SIS II legislative instruments? Are you satisfied with the transparency of the process and should there have been an impact assessment or public consultation? All three of you—and the same will of course apply to Professor de Roos when he is here—are welcome to answer any or all of the questions. Who would like to have a shot at that one?

Ms Brouwer: The Meijers Committee welcomes the fact that the European Parliament has been much better involved in the decision making on SIS II and not only with regard to the Regulation on SIS II but also with regard to the Decision. As we have seen in the last weeks, the LIBE Committee was able to decide or take a part in the package deal on two decisions. I think that is an improvement and you could say that this is a start for more transparent decision making. We are concerned however that there have been many decisions adopted between 2001 and 2006 on the actual use of SIS, extending the use, giving new authorities access to SIS, and broadening the functioning of SIS. This has already been incorporated now in the decision making on SIS II. This piecemeal approach, as it is called, is making for opaque decision making on this issue. Secondly, national parliaments and the UK Parliament have found it very difficult to cope with the different

amendments since the European Commission published the proposal in 2005. As you probably know better than we do, there have been many amendments from the Member States and, every time there is a new proposal from one Member State, it makes it very difficult to see what is really happening to such an important issue like SIS, as Professor Groenendijk mentioned. So, we are not very happy with the actual decision making.

Q76 ***Chairman:*** What about impact assessment? Why do you think that none was done in this case?
Ms Brouwer: That is a good question because, in 2004, the European Council decided that, for large IT databases such as SIS, there should be an extended impact assessment and there has not been one on SIS II. Professor Peers knows the decision-making process better in the third pillar framework but I think it would have been a good opportunity to make such an extended impact assessment. If you would allow me to say one more thing, the Meijers Committee has commented on the extended impact assessment on the Visa Information System. You cannot say that there was a proper balancing of the positive and the negative aspects of VIS. You could have doubts about whether this was the perfect assessment before reaching a decision on the Visa Information System, but it is a start.
Professor Guild: I would like to add a few comments as well from the perspective of ILPA. We note from the proposed Regulation and the Decision on SIS II which have now been agreed with the European Parliament that, rather than more transparency by the involvement of Parliament, what seems to be happening is that the European Parliament is being taken into the shadows with everybody else. They are agreeing in private negotiations and then what will happen is that the Regulation and the Decision will be adopted at first reading by the European Parliament. Therefore, instead of the Parliament necessarily increasing transparency, it in fact seems to be being drawn into negotiations behind closed doors and while we have a much better system of releasing documents, I am not sure that transparency is what is happening.

Q77 ***Chairman:*** May I interrupt you there and ask you: are you aware of complaints from the European Parliament at this lack of transparency?
Professor Guild: I do not know about complaints by them because they are involved. It is us—we are excluded. They are in, so they have stopped complaining, but we are not in. It is all very well and good but it does not solve the problem from the perspective of civil society. On public consultation, we notice that the European Data Protection Supervisor and national data protection supervisors in fact made a number of comments in respect of both of these proposals, but we do not notice that their comments having been received actually made much impact. We are somewhat concerned about whether, even if there is public consultation, consultation is being taken sufficiently into account. Is sufficient weight being given to those who are going to have the duty of enforcement? There seems to be a very heavy obligation on data protection supervisors to provide an intermediary control of SIS II. On impact assessments, I would certainly support what Evelien Brouwer has said. In my view, the problem about impact assessments is that so far they are done by the same people who are writing the proposal, so they are not independent, and they are designed to justify the proposal. Therefore, I am not quite sure why we are calling them "impact assessments", they are explanatory memoranda.

Q78 ***Earl of Caithness:*** Do you have any evidence that the current SIS has proved its efficiency and added value for maintaining a high level of security in an area without internal border control and, if so, what is the evidence?
Ms Brouwer: Your question is as to whether the current use of SIS works for improving security. That is a very good question and you would have thought this would be the first question to answer, when starting with the development of the second generation SIS. Is the current SIS actually functioning? I have not seen any document at the EU level or the national level where Member States or national police organisations are saying that security is much higher now and SIS works. I think that if you ask immigration law officers, they will tell you that it works because it is sort of efficient. From an immigration law point of view, I do not say that it works—and we will come on later to that—because there are a number of deficiencies. I think that immigration law authorities will tell you that we have a good system: that you put persons into the system and another authority in another country will know that this person has to be refused entrance. For policing and law enforcement authorities, at this moment, I have not seen evidence that SIS is giving added value and, from my research, I think that immigration law authorities will say that it is a very useful tool but only in a restricted sense.

Q79 ***Lord Avebury:*** Can you say anything about the impact of the multidisciplinary group on organised crime and its work on the European data protection framework on SIS II? To what extent does the work of this multidisciplinary group have an effect on the data protection regime to be adopted for SIS II? How did such a group come into being to look at these aspects of the European data protection framework?

Ms Brouwer: I think that would be a good question to ask Professor de Roos when he arrives. Do you mean the actual framework decision on data protection that has now been drafted and how that will work?

Q80 ***Lord Avebury:*** No, I am talking more about the process, the existence of the multidisciplinary group on organised crime and its role in examining the European data protection framework as it applies to SIS II.
Professor Guild: I would like to begin with a couple of comments in answer to that question. The first question was as to how these groups came into existence. I think that one of the grave difficulties we have in a variety of EU venues is a lack of a legal base in the introduction of different bodies. We create bodies and subsequently we may or may not create a legal base to which that corresponds. We have had this with the police chiefs. In fact, CEPOL had no legal base when it was set up. Yet it is all over the place, it happens endlessly, and I think you have identified one of those difficulties. We set up a body. Its membership is decided on a mix of political and executive decisions, and it is then let loose on a subject matter without any self-evident controls around what it is supposed to be doing, why it is there or to whom it is responsible, as one would expect if it had a proper legal base.

Q81 ***Chairman:*** Professor de Roos, you are welcome. I am sorry that you have had trouble getting here, but we are extremely grateful to you and to your colleagues for coming from Holland this morning for this session. I will now move on to the second question that I want to ask which is, does the agreed text of the regulation satisfy the concern about the accountability of the agency to be established to run SIS II? What other specific rules should be adopted to ensure accountability and should this agency have competence to run any other EU agencies? Who would like to have a shot at that?
Ms Brouwer: As you know, the management authority is now only a proposal and there is provision within the Decision and the Regulation that the Commission will publish a legal proposal within two years after their entry into force. We think there are only a few provisions which provide safeguards for the functioning of this management authority. It only allows the European Data Protection Supervisor to supervise the data processing that will be performed by this management authority. The view of the Meijers Committee is that there are only minor safeguards at this moment. We have of course to wait for the Commission's proposal on this issue. The four aspects which we think should be regulated in general, not only for the management authority for SIS but also for other independent agencies who are working within the framework of the EU, are firstly that there should be full competence of the European Court of Justice to assess the legitimacy and the lawfulness of acts performed by those authorities. The decision making and documents which those agencies and authorities are producing should be transparent. The same transparency rules for EU institutions should also apply for those institutions. With regard to liability, I think it is very important that there should be very accurate provisions on dealing with individuals harmed by data processing caused by the functioning of the management authority. There must be a good provision on assuring the liability of the management authority. There should be no gaps in legal protection.
Professor Guild: On behalf of ILPA, I would like to add a couple of points to what Evelien has said which we very much endorse. The first issue which concerns us is accountability to whom? What kind of accountability are we talking about? Is it political accountability, legal accountability, accountability to the police and immigration authorities, accountability to the data protection officers, or accountability to the individual? We have a variety of questions around accountability. We are very concerned that the weakest of that group of different categories of persons to whom accountability may be allocated are the individuals whose information is in the system, and therefore we would like to see strengthening of the measures of accountability to them. At the moment, it seems that there will be an indirect system of accountability via first of all a subcontracted agency, and the agency will be subject to the European Data Protection Supervisor and the national supervisors at the national level. We wonder whether this is really good enough to protect the individual.

Q82 ***Baroness Bonham-Carter of Yarnbury:*** In your written evidence, you say quite strongly that you are concerned about the setting up of new agencies. What would be your preferred way of managing the system?
Professor Groenendijk: As regards the Meijers Committee, it would make things a great deal clearer and solve a number of problems that Ms Brouwer just mentioned if SIS was under the Commission. If it was a Community agency, then all the rules on remedies, liabilities, and the general rules on transparency of the documents would apply, and I think that is exactly the only reason why it is outside! That is why we started talking about Schengen in 1990, because it was kept away from the control by the parliaments and by the judges. That is the only real reason that I can mention.

Q83 ***Baroness Bonham-Carter of Yarnbury:*** As I understand it, the Commission is going to start off running it; is that correct?
Professor Groenendijk: My impression from the documents I have read is that it will be an ongoing battle between the Member States and the Commission and this is a phase in that battle. I hope that, in the end, the same will happen that happened with the Schengen that was incorporated in the EU Treaty. For reasons both of efficiency and democracy it will be good, but this will be a long battle.

Q84 ***Earl of Listowel:*** Please forgive me if I am asking this question out of turn, but we heard last week that there is a team looking across Europe at how different countries access the information and checking that the access to information is secure. I think that you also said in your evidence that you would be interested in seeing better monitoring of who accessed the information, how often it is accessed and so on. That may come in our later questions but it does seem to bite on the accountability of what happens with SIS. Are you able to help me with information on those teams and how effective they are in actually checking that?
Ms Brouwer: I must admit that this is new information for me, so thank you for providing this information. I am not aware of teams looking at different countries. I think it would be a good opportunity if it is happening at this moment. I am only aware of the Joint Supervisory Authority which is functioning at this moment for the Schengen Information System, which has made some inquiries through the data protection authorities of the different countries into Article 96 on the actual input in SIS. And now there is an inquiry into Article 99 on the alerts for special searches. If I had come across the teams you are mentioning, I would be able to help you but . . .

Q85 ***Lord Corbett of Castle Vale:*** Would you tell us your particular concerns about the interoperability of databases.
Ms Brouwer: I can be very brief. There are two major concerns. The first concern is that it is absolutely contrary to the purpose limitation principle, which sounds like the old-fashioned principle of data protection but I think the data protection authorities agree with us that it is a central basic principle of data protection law, and it is important for protecting the transparency of the use of databases holding personal information. It is important for balancing the powers between different institutions and important for giving the person concerned information on how his or her information is used. I think that allowing interoperability is going contrary to this principle and it is a very critical argument. The second major concern is that it will affect the reliability of the information and it includes a risk of contaminated information. It is not very difficult to understand that, if you allow many organisations to use the same information and the same information goes through one database to another database, then different databases will become contaminated if the basic information is not reliable, and we know from the practice of the Schengen Information System that the information which is reported by the different national authorities at the local level is not reliable all the time. I am very concerned about this principle of interoperability and about the proposals stating that we should connect Eurodac with VIS and VIS with the Schengen Information System, and to Europol, and Europol can transfer data further to third parties and third countries. I think that is a major problem for my Committee.

Q86 ***Lord Corbett of Castle Vale:*** We have problems with the accuracy and motivation of the police national computer. There is a high level of inaccuracy in those records.
Ms Brouwer: Exactly, and that is what you hear from all the countries. In France, there are complaints about the reliability of immigration data bases and, in Germany, the Federal Police are laughing about the immigration administration because everybody knows that the immigration administration is not very reliable and causes problems. In the Netherlands, we have the same problems. Thinking about the impact of the Schengen Information System II, which will be applicable in more than 28 states now that we have Bulgaria and Romania joining the European Union, ,I think it is a very important problem.
Professor Groenendijk: From the study which Ms Brouwer is writing right now for her PhD, it appears that in France 40 per cent of cases where the French Data Protection Authority checked individual registrations in SIS they were either incorrect or unlawful; and, in the reports of the Data Protection Authorities of the German Länder, the percentage of registrations which were unlawful, records that were not allowed under the present Schengen rules, included between 10 to 50 per cent. of the data. The present proposal is to use these kind of data for completely different purposes with far-reaching consequences for individuals. I think it is a risky affair.
Chairman: Professor de Roos, I should have repeated what I said at the beginning of the session before you were here and that is, please, feel free to intervene whenever you want or at least to invite yourself to intervene. The reference to incorrect data takes us straight on to the next question about biometrics.

Q87 ***Lord Dubs:*** From the written evidence, it seems to be your view that the use of biometrics as identifiers should be ruled out entirely, that is identified on a one to many comparison basis. I looked at the evidence and you seem to have two sets of concerns, one is about technical reliability—or should I say technical unreliability—and, secondly, privacy and human rights concerns. Would it not be enough to have adequate safeguards for the use of biometrics? Secondly, do you have similar concerns about the use of biometrics for verification, that is to say on a one to one comparison?
Ms Brouwer: Thank you for the question. The two concerns you quoted were its reliability and the human rights impact. I think I could add a third one which is the security of biometrics. I think there are those three problems. As regards the reliability, many data protection authorities and also IT specialists agree with us that it is not clear at this moment which procedure of biometrics—fingerprints, iris scan or facial recognition—gives us the maximum guarantee of reliability which will be 100 per cent right. A one to two per cent false rejection rate or false acceptance rate for biometrics is considered normal and this means that introducing these data into databases where the data on millions of individuals will be stored, will mean that a huge number of individuals will be permanently accepted or rejected wrongfully. The second problem is the security of biometrics. It has been proved last summer by IT specialists that biometrics are not secure; they can be stolen or there can be fraudulent use of biometrics by criminal organisations or by other specialists. There could be unauthorised access to the documents on which biometrics are stored. I think that, as long as those problems remain unsolved, it is too early to think about safeguards. I think that you should first of all be sure that biometrics are reliable and secure, before developing a central database of biometrics. However, we have thought about possible safeguards because we know that the policy will not stop by introducing biometrics. We agree that there should be safeguards like fallback procedures if somebody is rejected at the borders. Also, there should be a procedure whereby one decision that your biometrical features do not match the registered data, is not enough to deny someone their rights. But we have a principal objection against the decision to start running the central database for biometrics and then say that the safeguards will come afterwards. We agree with those institutions and specialists who say, "No, first think about what you are doing and then start applying it in practice".

Q88 ***Lord Dubs:*** I understand what you are saying in relation to the use as identifiers, that is to say one to many comparisons, but if you are looking at the use of biometrics for verification of other information, then surely some of your objections would have less substance.
Ms Brouwer: I agree with you that it makes a lot of difference what kind of use is intended with biometrics. Is it just for verifying whether the person carrying the identity card or passport matches the information stored on the card. or only to see if the person who is presenting himself is the same as registered on the card? It might be that a central registration in future provides an extra tool to safeguard just for this verification: is this the same person as the person who has applied for a visa or for a passport? But in the case of the Schengen Information System II, the policy makers are considering using biometrics as a search tool and I think that will have a much larger impact. It is not one to many, it is just using biometrics for searching in different databases, "is the person we are looking for registered somewhere?". If there are problems on security and reliability, I think that is a much larger concern.

Q89 ***Lord Dubs:*** It is going beyond the bounds of our inquiry, but you seemed to have undermined the American policy on biometric information on passports and British Government policy on identity cards, but that is not what we are talking about today.
Professor Guild: May I add a couple of extra comments that are from a slightly different angle for ILPA. The first is, what are we seeking with biometrics? What we are seeking with biometrics is in fact security about the individual and the document. The difficulty with that is that it is a never ending search. You will never get to the point where you are absolutely satisfied, no matter what biometrics you use. You can even use DNA but there is always the doubt; there is always the search for further security that the person holding the document is indeed the person who is entitled to it. We could get to the point where we are tattooing people's arms but do we want to go there? Is this what we want to do? Do we want to say, we are willing to accept a degree of insecurity as regards the identity of the person in the document? I think that is the first fundamental question which we have to answer.

Q90 ***Lord Avebury:*** You have some experience with Eurodac on false policies. If we look at the number of occasions somebody has been wrongly identified as of interest to the immigration authorities because of incorrect recognition of his fingerprints on Eurodac, then that would presumably feed across. You talk about a 1 or 2 per cent error but I did not think that it was anything like as high as that in the case of fingerprints.

Ms Brouwer: I am not aware of the percentage of mistaken identifications in Eurodac.

Q91 ***Lord Avebury:*** Would it not be important to look at that?
Ms Brouwer: Yes, I agree that it would be very important. I think the problem with using biometrics in the field of immigration law is that differentiating between applying biometrics for the use of EU citizens for their passports and identity cards or for controlling immigrants, for questions such as: "Do we want him or not? Can we expel him?" Immigrants are not so aware of their rights and the possibility of going to appeal and say, "You must be wrong, I am not the same person". Somebody using a false passport is another problem. I am not aware that Eurodac will give you the percentage of people who have caused this problem of wrong identification.
Chairman: I should perhaps say on this as on any other question, if any of you think when you see the transcript that there are additional points that you ought to make to us in writing, we would be very happy to receive them.

Q92 ***Lord Avebury:*** I would like to ask one more question on that topic. Surely, if there were false identification of people as being of interest to the immigration authorities, then we would have known about it, because those people, having been refused entry at a particular border, would be vociferous in their complaints about the false identification. It is almost certain that each individual case of error under Eurodac would be shown up through the complaints which the individual or their representative would no doubt make to people like us or their Member of Parliament.
Professor Guild: The poor people who are in the Eurodac database are amongst the most vulnerable who exist and their access to lawyers or to anyone who will help them to make a complaint is extremely weak. If we take the example of a case which came before the High Court here, it was after a number of similar cases where the UK authorities had sent back to other Member States, particularly to Italy, asylum seekers for whom they said they had a positive match of fingerprints, and they sent back the wrong person, and the Italian process is that the person cannot then make an application for asylum because they are excluded because they have made an application in the UK, therefore they are excluded from any benefits. These people were camping in the grounds of the Italian Refugee Council and it was after numerous of these cases that finally the Italian Refugee Council got in touch with the Refugee Council here and they started a case in the High Court to require the Government to bring these people back to the UK. Yes, the fingerprints matched in the system, but the individual who was sent back was a different one. They just picked up anybody out of detention and sent them back—"Oh, you are a Somali, Mr Ali, we will send you back, you must be the right one"! It went on for months. Within the system, even with the fingerprints matching, the wrong person can be sent back regularly. These individuals have so little access. Most of them are sent outside the Member State with summary procedures. How many complaints will get to you?

Q93 ***Lord Dubs:*** I would like to move on to another question altogether. With regard to the draft regulation, you seem concerned by the vague criteria for the inclusion of data concerning third country nationals to be refused entry, which you say will continue to lead to different interpretations from one Member State to another. What specific harmonised rules should govern the grounds for issuing alerts on third country nationals to prevent this?
Professor Groenendijk: As to the last question, the Commission originally made a proposal to limit the possibility to register third country nationals in the Schengen Information System for certain specific crimes only and, from my recollection, they referred to the list of crimes under the European Arrest Warrant. If you limit registration to certain specific crimes, it will be much clearer than now. The only threshold is a maximum penalty of one year threatened under national law for any infringement of immigration law. I am afraid that all of us have once upon a time infringed the immigration legislation of another country. I think that specification would be the answer. As to the problem with third country nationals, I think there are basically three categories. First, the third country national family members of EU migrants who have under community law a right to live with their EU family members in a Member State. In Article 15(a) of the proposed Regulation, there has been a solution along the lines of the ECJ judgment in *Commission v Spain* that was decided earlier this year, where Spain had refused a visa and the right of entry to two third country nationals who are family members of EU citizens.because they were registered in SIS by Germany. Spain was told that it should have used its SIRENE contacts to check whether there was a real danger serious enough to refuse the entry or the visa. This might be a practical solution in visa cases but in practice it does not work at borders. Before the border authorities have contacted their capital and the capital has contacted the other capital and they have contacted the SIRENE Bureau, many flights will have gone and many more hours will have passed. For this limited group it is a solution, but I think there is a second group of third country nationals who, under the new directives on legal

migration, especially the family reunification directive and the one on long-term residents, have a Community law right to remain in the Member State. This group is completely disregarded. In our view, they should be excluded from the personal scope of this Regulation altogether because what you will get is people, third country nationals, who will have a long-term residence permit under the directive and then they can still be registered sooner or later in the SIS II. At the time of drafting that article, the granting of residence permits and the withdrawal on public order grounds was still a completely national issue which it no longer is, because now both the issue of granting or withdrawal of residence permits for family members and for long-term residents are community law matters. So, what we are in fact getting are two sets of rules and criteria, one in this new Regulation with very low thresholds and, in the directives, you grant a right with only very limited possibilities to withdraw this title and to refuse people at a border and this is completely disregarded. I think the drafters have forgotten this category. More than half the third country nationals live in the Member States or at least in a Member State where those directives apply, so it is a pretty large group. There is a nice rule in Article 20AA of the SIS II Regulation which has been more or less copied from Eurodac which says as soon as a third country national acquires the nationality of one of the Member States, the Member State who made the registration in SIS should take care that these data are deleted; but who knows? In Eurodac, there is a rule that as soon as a third country national gets a residence status or the nationality of a Member State, his data should be removed from the system, but the national authorities which grant nationality never think of warning another Member State that they should remove their alert. This is a provision that looks very interesting and fair but there is actually no implementation of it. Large numbers of third country nationals are registered in SIS and will be registered in the SIS II. We see that already right now Member States have a problem removing from SIS data on people who are notified as being EU nationals from the system. We have a system that failed to produce the data that they are EU nationals and thus should be removed, but of the large group of new EU citizens, nobody will know, and the system surely will not know that they are EU nationals and should be out of the scope of the system. On that point, the draft regulation is really deficient in our view.

Q94 ***Earl of Listowel:*** Have you any comments on the listing of third country nationals, including on foreign policy sanction lists, such as the UN Security Council travel ban, and do you have any further comments on family members of EU citizens? I think you did approach that fairly thoroughly in your last response.

Professor de Roos: We are fairly concerned about that, if you recall this example of the United Nations terrorist lists. There is no control on that whatsoever and that is a huge problem. There was a judgment of the European Court of Justice on 12 July 2006 in which the Court made clear that Member States should provide for accessible remedies to individuals to make it possibly to apply for a re-examination of listing by the Sanction Committee. I think that is essential. There has to be a control and there has to be an effective remedy. If you miss that then misrepresentation of this sort of information could play a role. Maybe I could put this in a somewhat broader context. We are wrestling in our country, but I think the same goes for all countries of the European Union, with the problem of information stemming from the security services and information gathered by judicial authorities. Now we have some brand new legislation which is not working yet but will be able to be used in our country to make it possible to interrogate witnesses against the accused, witnesses who are working for the security services. It is a hell of a job to make that compatible with Article 6 of the Human Rights Convention, the fair trial provision. There has been an effort to make that control a little bit possible, but the problem remains that the function of security service information is completely different from the function of judicial information. Judicial information is gathered in order to find the truth and then put the accused to trial, and see to it that there is a fair trial as well, of course. That is one thing. The other thing is that for the security services it is not really important for them to go into procedural truth-finding, but they want to know what is going on and work on it. In the end, if there is a link, if there is a serious risk of committing an offence or making plans to commit a serious offence, then of course the security services have a duty to get the information through to the judicial authorities. That is in an extreme situation. We have had some trials in our country and our experience is that criminal trials in which security service information plays a necessary role are quite hard to handle. We have had acquittals and now there are some procedures in which the idea is to use information gathered by the security services. As this is not in itself reliable information or information that can be used in a fair trial. That is a general problem which also plays a role, I think, in this context.

Q95 ***Lord Avebury:*** You made a comment about remedies for individuals put on this list. Can I ask about a particular case of persons who are declared non-conducive to the public good, and I believe there

is a category similar to that in many other European countries, but that is how we describe it in our law? Those people never have a right to challenge their inclusion on the list which is promulgated by the Home Office, and I presume the same is true in France, Germany, et cetera. Are you suggesting that they should now have such a right as part of the Schengen system?
Professor Groenendijk: I would respectfully disagree. I think this category is a typically British one, at least under the system of immigration control. I know that in our country under the immigration legislation, if any non-citizen that is on the point of being expelled or of having his residence permit withdrawn, even if the legislator has tried to reduce his remedies there is access to court. The civil courts in our country have accepted the task of allowing at least one form of a day in court in these kinds of cases. There is always a remedy, either in immigration law or in the general administrative law, and if both fail there is a remedy in the normal civil court. It is not possible for the Dutch Government to expel somebody without him having at least an hour or so to apply before a judge.

Q96 ***Baroness Bonham-Carter of Yarnbury:*** Are you aware of SIS immigration data used by relevant authorities in other Member States for the purpose of determining the merit of asylum applications and, if so, what are your concerns about this?
Professor Groenendijk: In order to be able to answer this question I contacted the Dutch Refugee Council, and since they were unable to be of help I contacted a colleague in Austria. She gave almost the same answer I would have given for the Netherlands, that the Dutch authorities deny that they do so, and it is unclear whether they actually do it. I could mention two occasions in an asylum procedure where authorities would be interested in checking with the Schengen Information System first for the application of the Dublin Regulation. Is there another country that has already registered? Of course, it is unclear whether it would be a useful idea, because this is not mentioned under the Dublin Regulation as proof of an asylum seeker having been in the other Member States that have registered him in the Schengen Information System. The other moment is at the very end, at the moment when the immigration authorities are on the point of granting refugee status. Then I think, implicitly under the Schengen Implementing Agreement, they are under a duty to check whether this person, the third country national, has been registered by another Member State, because then either the alert has to be removed or the residence permit has to be refused. That is in Article 25 of the Schengen Implementing Agreement. I think the Commission originally also considered the possibility of expanding the access by the asylum authorities to SIS, but I think Member States now are more interested in using VIS for this purpose because evidently there will be a lot more data, a lot more persons who will be registered under VIS than under SIS. That is also the answer from my Austrian colleague, that for the time being Member States do not want to have access for asylum cases through the SIS because they are thinking about VIS. But this does not say anything about the actual practice whether they are using it right now for that purpose.

Q97 ***Baroness Bonham-Carter of Yarnbury:*** But you do not have concerns about their use of VIS rather than SIS?
Professor Groenendijk: Our concerns would be the same as already have been formulated by Ms Brouwer, that the data are so unreliable. I think that makes the system also not very effective for Dublin purposes because the data in the system are so unreliable.

Q98 ***Earl of Caithness:*** Can I follow up what Professor de Roos was saying about the security services? There seems to be a disagreement between the Council and the European Parliament on this. Could we have a bit more of your thoughts on whether the SIS II data should be available to the security services, and do you differentiate between the security services in the Schengen countries, the security services in the non-Schengen but EU countries, and what I would call the third parties, all the other security services? Do you envisage a situation emerging with SIS II which happened with the similar system where the CIA would get involved with our friendly Belgians?
Professor de Roos: As I have already many concerns about the use by Schengen countries of this information and the combination of criminal law information with security service information, the more I have concerns about the CIA having access. I have the impression that the way the CIA works is rather rough as compared to our European methods. For instance, we have FBI officials working with the knowledge of our judicial authorities. That is okay, but then immediately you see that the FBI methods are dramatically rougher than not only the continental but also the British ways of working.
Ms Brouwer: I am concerned about the proposal. I am aware that Germany is now trying to include it in a compromise text as agreed upon by the LIBE Committee in the European Parliament. There should be access for internal security agencies not only to criminal law information but also to information on immigrantsI think it is institutionally wrong to include this information in the Decision as it will concern the use of information which is regulated in the Regulation. Secondly, exactly as

Professor de Roos and Professor Groenendijk are saying, internal security agencies using this information which is stored in SIS for other purposes cannot be further controlled. Why? Because we accept that there is less control on how security agencies are working. This means that you lose control on how the information is used. With regard to your question on the use by third parties, bilaterally information is already shared between security agencies and between the police and other authorities in the United States or other third countries. One of the problems with the Schengen Information System, and the problem we were referring to at the beginning, is that there is no transparent all-round view of what we are dealing with. For example, Member States have readily provided Europol with direct access to SIS information and we know also that Europol already has bilateral agreements with the United States and authorities in the United States for further data processing, so it is very easy to see that information stored in SIS II will find its way to the United States. It is one of the problems which should be dealt with more elaborately within the national parliaments but also at the level of the European Parliament.
Professor Guild: May I add a comment from a slightly different perspective? The first issue which one would have to accept is that if an individual's information is in the SIS II that will be a presumption that that person has done something wrong. You have in all the mechanisms by which the individual is put into the system a presumption against them. Once you have a presumption against the individual, the wider you spread the presumption around the world the worse the consequences are for that individual. We have already discussed the question of how you get into the SIS, and there have been substantial concerns raised about the extraordinarily flexibility of the criteria on the basis of which somebody may be registered in the SIS, and the very wide degree of discretion which is left to a particular Member State official to insert someone's information into the SIS. The consequences of that are amplified when that information is then passed around. We are concerned about two things in particular in relation to these databases. One is fishing and the other is data mining. One is going in and trying to find something about somebody and fishing around in different databases to pull out bits of information to construct some kind of a bigger picture of suspicion in order to justify or support concerns about an individual, and the other is having a profile of what you are looking for and seeing who out there fits that profile. Both of these techniques are very widely used by the security services. There are much greater limitations on these techniques within the police and judicial authorities. We have had the decision of the German Constitutional Court prohibiting the use of data mining, but security services, because of the consequences of the type of work they do, use (and probably use justifiably) these mechanisms, but then to give them access to a database which raises suspicions on very limited grounds seems to me to be an error.

Q99 ***Earl of Caithness:*** How do you control it? Any suggestions?
Professor Guild: How does one control data use? Quite simply—you state that they shall not have access. Access will be limited. This is one of the problems that we spoke about earlier, about interoperability, and, of course, the EU's principle of availability. Availability to whom and under what circumstances? These are issues which we have to be very careful about because they are at the heart of due process and democracy.

Q100 ***Baroness Henig:*** Do you think there are any exceptional circumstances in which data collected for one purpose for SIS should be used for another purpose?
Professor Groenendijk: Yes, but then they should be very clearly described and formulated in the Regulation. I think purpose limitation should be the guiding principle first, only immigration data for immigration authorities, only police data for criminal prosecution purposes. Of course, you could imagine that for very grave acts there would be an exception made, but now what they are proposing is to store more data on more people and give more institutional access without any real limitation. I think the relatively limited number of occasions where we would all agree that there was a need to use any data possible could very well be described. If that was really what we wanted that could be described and those crimes could be mentioned in the Regulation. That would then be the exception to the rule, but now the rule has become that purpose limitation is not enforced any more.

Q101 ***Baroness Henig:*** So in fact you can cater for exceptional situations by much clearer and tighter definitions is what you are arguing?
Professor Groenendijk: Yes, but we have done away with the principle so you do not need to specify or justify anything any more because everything is allowed.

Q102 ***Lord Corbett of Castle Vale:*** You may well see this as special pleading, but here goes. Do you believe that the UK should have any access to SIS immigration data, at least for purposes related to asylum determination, responsibility or security? In

turn, of course, that would mean we could share what information we have with other EU states.
Professor Groenendijk: The way the question is formulated, "should", means it can be interpreted as a political question: is it desirable, as a legal question: is it lawful right now, or as a practical question: is there any use for it?

Q103 ***Lord Corbett of Castle Vale:*** Does it make common sense, is what I mean.
Professor Groenendijk: On the legal question, the Legal Service of the Council has given a clear answer to that question, No under the present rules, but it has added as a kind of footnote that of course there can be bilateral contacts between Member States, which would, I think, solve most of the British worries. If there is real need there is a bilateral solution. If you take this as a political question I think the question can be seen on two levels of the relationship between the Member States. Is this a kind of free rider behaviour of one Member State who just wants to use systems developed collectively if it is urgent or if it is useful? Should that be honoured or stimulated? You can also look at it on the question of individuals. The Schengen Information System originally was designed as a compensatory measure because of the free movement of all persons living in the Schengen area, so what would happen if you allowed one Member State not part of the Schengen group to use SIS against third country nationals? For them this free movement is a real, very important advantage, that they are not checked at all the internal borders because of their origin or because of the colour of their skin. So doing away with the internal border controls was a great advantage for third country nationals. What Britain says is, "We want to use the system against certain third country nationals without giving the large group of third country nationals the advantage". I think that is a question of fairness and on that level I would have my doubts.

Q104 ***Lord Corbett of Castle Vale:*** You are aware that all this was suspended for the World Football Cup and internal border controls were reintroduced?
Professor Groenendijk: Yes, for a few weeks.

Q105 ***Lord Corbett of Castle Vale:*** It does not matter for how long, does it?
Professor Guild: On behalf of ILPA I have to make a comment on this particular question. On the one hand you have the perspective from inside Schengen. From the perspective of an association in the UK we would say that if there is not the right of free movement without a border control there is no justification for access to a flanking measure to limit free movement and therefore the UK should not have access to the SIS unless or until it is willing to lift its internal border controls with the other Member States.

Q106 ***Earl of Caithness:*** If I can go back to Baroness Henig's question, can I ask whether you have suggested a redraft of Article 17A to the Commission which, as you state in your evidence, says, "Users may only search data which they require for the performance of their task"? If you do not think that is strong enough have you suggested a redraft?
Professor Groenendijk: I am afraid that we are unable to answer the question right now but the Lord Chairman has already given us the possibility to have second thoughts on our way back, so maybe we should use the opportunity.

Q107 ***Lord Corbett of Castle Vale:*** Phone a friend!
Professor Guild: The key is in the question, of "users". It is the definition of who are those users and I would wish to see a very narrow definition of the users and then we would not need to redraft 17A because the users would be specified by their function and their function would determine what the performance of their tasks would be.

Q108 ***Lord Avebury:*** Returning to the question of the data protection rules in the SIS II legislation, and in particular to the discussion in your paper on whether the Data Protection Framework Decision should be made applicable to SIS II instead of having specific to SIS II data protection rules, you entered a *caveat* that the Data Protection Framework Decision should conform to the highest data protection standards which are to be used for this purpose. I want particularly to ask you whether you have had a look at the document presented by the Council to the Multidisciplinary Group on Organised Crime that was published on 19 September, document 12924/06, in which they address ten questions to the Multidisciplinary Group, all of which appear to be directed towards watering down the standards of data protection. This document was not presented transparently in the first instance, although it is now on the Council's website. Have you any comments to make, first of all on the process by which this fairly far-reaching change in the Data Protection Framework Decision has breached the decision-making process through the Multidisciplinary Group, and, if you think that were it to be implemented, the Data Protection Framework Decision would maintain the highest standards that you call for in your paper?
Ms Brouwer: If I may start with your question on the Framework Data Protection Decision, first I have to admit that the Meijers Committee did not comment on it, although I think it is a very important draft, and

I discovered like you the latest draft now being considered of the Framework Decision. I agree with what you said at the European Parliament a few weeks ago, that we should not rush into accepting the text as it is now laid down. It is a very important issue for national parliaments and the European Parliament because we are considering the level of protection which is included in this draft. As SIS II is now to be postponed, we should take more time to further rethink and redraft this text. You put it rightly: you should not expect the Multidisciplinary Group on Organised Crime to present a data protection text. Our general concern, when we were referring recently to other documents, is that it gives the impression that it is dealing more with broadening the use of personal information and allowing national authorities to exchange this information within the EU territories. It also enables the transfer of data to third parties, which covers a very large part of the current proposals. We think that the proposal is more concerned with providing national authorities with the ability to communicate information rather than enforcing the rights of individuals. Therefore, with regard to applying this immediately to the Schengen Information System, we do not think at the moment that this is giving adequate protection to persons on this database. I refer to what has already been said by the European Data Protection Supervisor and the European Commission, that the level of data protection to be applied to the Third Pillar and to SIS, should be in accordance with the EC directive 95/46. Although this EC directive is also not ideal, it should be at least the minimum level and we should not go below it. What I have understood from the negotiations, is that some Member States even want to consider the protection of this Framework Decision as a maximum, so Member States should be prohibited from giving more protection in their own national legislation. I am very much concerned about that and I very much hope that in the national parliaments and also in the European Parliament there will be opposition against this principle of a maximum level. I agree with the Commission and with the Data Protection Supervisor, and it is also has been underlined by the European Court of Justice, that the EC Directive is a minimum level. As we have recognized data protection as a human right in the EU charter, I think we should not do away with the rights individuals have in these texts.

Q109 ***Lord Avebury:*** So you agree that if you have a grievance case you could get this right theoretically because of postponing the SIS II until 2008, which removes the urgency from getting European data protection programme as you would like to see it? If that is so, is there any way in which we can detach the job of looking at data protection for SIS II from a group described as the Multidisciplinary Group on Organised Crime, which is clearly an incongruous body to consider data protection and which we do not even know has any data protection experts serving on it. How does one go about removing the responsibility from that group and allocating it to some sort of body which would have data protection expertise?

Professor Groenendijk: Maybe we could learn from the experience of the negotiations on the Schengen Implementing Agreement when it was a group of national data protection authorities which sat together and were able to influence the negotiations at that time to insert the provisions on data protection in the Agreement that we have right now. It was these people who took the initiative to get attention for data protection, and I think with reasonably good results for the time, considering that it was 1989–90.

Professor Guild: I would just add that, of course, this problem is one of the constitutional structure of the European Union. It is because we have these pillars. We have been trying to get rid of them for a number of years now, not very successfully. The Commission suggested using the passerelle and the Finnish Presidency kicked off Tampere II saying, "Let's do it". This makes me wonder whether perhaps by 2008 we will. If we have, that means that instead of these two documents everything is going to be collapsed into one, and the key is going to be to ensure that the Data Protection Directive is the model and that will apply to everything. If they do not manage to finalise all of this and then try and bring it into a one-Pillar collapsed structure there will be unsatisfactory standards applying to certain areas. The difficulty is that managing an EU with the current structure is extremely difficult.

Q110 ***Baroness Henig:*** Do you have any comment on the future use of SIS II for police and criminal law purposes, including the operation of the European arrest warrant, and what problems in practice have there been to date with the use of SIS I for law enforcement purposes?

Professor de Roos: Let me say in the first place that SIS I is not the answer on the whole line, of course. It contains very useful elements and also protection for the individual, for instance. On the prohibition on double jeopardy, we have now this very important decision of the European Court of Justice in the case of *Van Straaten* (a Dutchman) *v Italy*. The Court ruled rather restrictively on this principle, or maybe you should say extensively in favour of the individual, where the formula was the identity of material facts, so not the legal label of it but the material facts identity and then a set of facts which

are inextricably linked. If that is the case we have to look at cases of drug trafficking between Italy and the Netherlands, for instance. Then, even if the amounts of drugs were different or the persons involved in the two countries were not the same, also in those situations, if there is a restricted link between the two criminal procedings, this could be the same case. It is prohibited to prosecute the person again in Italy when the person, Mr Van Straaten in this case, was already brought to trial and acquitted for this in the Netherlands. Now our concern about the future, if I may repeat what we have already said, is that if the information is entered into SIS II with all those alerts on rather vague grounds in a very extensive field, it will not be reliable. Then you have a problem, not so much with the use of evidence in criminal trials, but also with people who are under secret surveillance or with other kinds of investigative methods used by the police on grounds that are not very clear, or based on sources which are not reliable. That is our main concern.

Q111 ***Chairman:*** May I thank all four of you very much indeed for your extremely helpful answers to our questions, and indeed I repeat our thanks for your written evidence. I wonder if I can just ask a question, because Professor Groenendijk was very kind earlier on in the meeting in saying that to his knowledge we are the only Parliament that conducts inquiries of this sort. Have you been invited to give any comparable evidence to the Commission? Do the Commission consult you, any of you? Perhaps that is an impertinent question.
Professor Guild: When there are consultations the Commission normally sends us an invitation to submit to them our position and they usually open some arcane website somewhere and put all the evidence on it, and if anyone is interested they can look at it, and one rarely gets anything other than a little notice back thanking you for your participation. One certainly does not have the sense of the careful scrutiny of witnesses specifically chosen for their expertise on a particular aspect in a setting like this with the assistance of experts which your Committee does. Certainly I have not ever had the impression that the European Commission has sought to ask me specific questions to seek specific answers and in fact to test my answers and the evidence which I have given them in the way in which your Committee does.

Q112 ***Chairman:*** How about the European Parliament?
Professor Guild: In my experience of the European Parliament it is developing a system of using external experts on particular subjects. However, my experience so far, and I have only given evidence once to a committee in this context and that was only a couple of weeks ago in Brussels, is that it is very much in development. It is not nearly as developed into a system as you have here.
Professor de Roos: They are asking questions now and then on important issues, of course that happens.

Q113 ***Chairman:*** In so far as you have ever been asked questions by either the Commission or the Parliament, are you aware of changes in the process of Green Paper to White Paper that have taken account of your comments?
Professor Guild: It would be very difficult to point specifically to one particular change which has happened. A colleague of mine recently said in a public venue that the proposals which she had put to the Commission for the production of the Hague Programme had all been taken on board in the Hague Programme. I listened to this with astonishment.

Q114 ***Lord Avebury:*** As a corollary to that question I was going to ask whether you have been asked for any advice by the Multidisciplinary Group on Organised Crime and whether you know of any other civil society organisation that might have been consulted by the MGOC.
Professor Guild: I think they may not be aware of my existence, as I am only vaguely aware of theirs.

Q115 ***Chairman:*** Professor Guild, I think it is extremely unlikely that anybody is unaware of your existence, but I hope that if there are any gaps in public knowledge our report will fill them.
Professor Groenendijk: I fully agree with everything that Professor Guild has said on this issue. I think the European Parliament is genuinely trying to develop methods of involving civil society and, as for the Commission, the only external parties that they systematically consult and discuss with when drafting a proposal are the civil servants of the Member States. They are involved in the drafting stage in a rather structured way, but apart from opening up a website and giving the opportunity to file notes before a certain date, I have no experience of it.
Chairman: Again, may I thank the four of you very much indeed for coming. Your answers have been extremely helpful to us. Professor de Roos, as I think I may have said before you arrived, you will receive a transcript in due course and of course you will wish to check that it is correct, but again I repeat that if any or all of you, on reading the transcript, realise that there are things that it would be helpful for us to have as supplementary evidence, we would, of course, be very happy to receive it. On which note may I thank you and wish you a safe and rapid journey home.

WEDNESDAY 25 OCTOBER 2006

Present	Avebury, L	Dubs, L
	Bonham-Carter of Yarnbury, B	Henig, B
	Caithness, E	Listowel, E
	Corbett of Castle Vale, L	Ullswater, V
		Wright of Richmond, L (Chairman)

Examination of Witnesses

Witnesses: MR PETER THOMPSON, Head of European and International Division, and MS HARRIET NOWELL-SMITH, Legal Adviser, Department for Constitutional Affairs, gave evidence.

Q116 ***Chairman:*** Good morning, everybody. Thank you very much for coming to give evidence to us. I will later, more formally, welcome those who are coming for the second session of our evidence; nevertheless, you are all very welcome and we look forward to hearing from you as well. I should first of all say that this is on the record. It is being broadcast by radio, not by television. For the record, I should say that this is part of an inquiry which this sub-committee is doing into SIS II, Schengen Information System II. I would like to start by asking you the first question. Before I do so, may I, through you, thank Baroness Ashton for her written evidence of 4 October? It was very helpful, and we look forward to seeing Baroness Ashton at a later stage in our inquiry. The Government refer to the power of the European Data Protection Supervisor to supervise the Commission's management of SIS II. Are the Government content—is your department content—with the inability of the European Data Protection Supervisor to bring proceedings within the Third Pillar, or proceedings against Member States which will be operating the system, or against a European Union agency as regards SIS II? I am sorry, it is a rather complicated question but I think that you have had notice of it.
Mr Thompson: We have indeed.

Q117 ***Chairman:*** Can I say that if you would like to make any opening statement, you are very welcome?
Mr Thompson: I do not have any opening statement in mind, but I wonder whether it would be helpful if we said a little about who we are and what we do, because I think that may help you in terms of the questioning. My name is Peter Thompson and I am Head of the European and International Division in the Department of Constitutional Affairs. My division is responsible for the strategic co-ordination and oversight of all of the department's EU business. So I am familiar with EU work across the piece here.
Ms Nowell-Smith: I am Harriet Nowell-Smith. I am a legal adviser in the DCA, advising principally on the negotiations of the Data Protection Framework Decision, and obviously we work on SIS II as well.
Mr Thompson: The question you raise, as you say, is quite a complicated question. The simple answer is that we are content with the arrangements that the EDPS cannot bring proceedings under the Third Pillar and, indeed, the EDPS itself has never had powers where it could actually initiate proceedings against Member States. We say we are content because we think that there are adequate provisions for the kinds of issues that might arise here in the instrument as a whole. Perhaps the best way I can illustrate that is briefly to go back to the structure of the database itself and the supervisory arrangements. As I am sure you are all aware, the SIS II database consists of a central database, which is actually located at Strasbourg but it could be anywhere, and a series of national databases in the participating Member States. The data in those databases is the same. They are all real-time copy updates. The national supervisory authorities—the Information Commissioner, for example—have Third Pillar powers and can of course initiate proceedings. Because the national supervisory authorities like the ICO can initiate proceedings, we are therefore happy with that kind of system because we think that proceedings are much more likely to be initiated at a Member State national level than they are against the central database, which is really just the hub of this system but containing the same information. The last point I would want to make is that the Council decision provides for mechanisms whereby the national supervisory authorities like the ICO and the central supervisory authority, the EDPS, can co-ordinate their activities and address cross-border issues. From memory, it talks of meetings between them twice a year. For all those reasons, therefore, we think that the arrangement, though perhaps complicated, is satisfactory.

Q118 ***Chairman:*** We of course are not Schengen members. Are you satisfied with the extent of co-operation and consultation that we are involved in over the process of SIS II?
Mr Thompson: We are rather complicated here, as we are not Schengen members for the immigration data but we are members for the police and judicial

co-operation element of the data. That is clearly a complicated situation. Certainly we have no evidence to suggest, in the discussions that there have been about SIS II—though we have an interest in the data protection element of SIS II, the lead department is very much the Home Office, with whom we work very closely on this—we have no reason to believe that those discussions have been anything other than satisfactory.

Q119 ***Chairman:*** What about judicial control over the agencies? The rules governing the access of Europol and Eurojust to SIS II data—is there adequate judicial control, do you think?
Mr Thompson: We think so. Here again, from memory, Articles 37A and 37B—I may have to correct that as we go along—set out the rules governing Europol and Eurojust, in terms of how they can access the database and what they can do with the data. We think that those are appropriately rigorous rules. So that gives us comfort. It is also worth saying that both of those bodies are well-established, well-respected bodies, set up under their own detailed legal instruments. As I said, the Council decision sets out a wide range of rules that they have to abide by when dealing with data. Equally, Europol and Eurojust—although again this is very much a Home Office lead and I am not an expert on the bodies themselves—as I understand them, are very much information hubs. They would not be acting on the SIS II data themselves; they would merely be making the connections to bodies that would act on that data. I hope that is not too round-the-houses, but we think that the rules governing Europol and Eurojust are appropriate and sufficiently rigorous.

Q120 ***Chairman:*** Incidentally, if there are any legal postscripts you want to make to Peter Thompson's evidence, you are of course very welcome to give them.
Ms Nowell-Smith: Thank you.

Q121 ***Baroness Bonham-Carter of Yarnbury:*** I want to clarify one thing. You said the central database and the national database have all the same material. Is that right?
Mr Thompson: Yes.

Q122 ***Baroness Bonham-Carter of Yarnbury:*** As non-members of Schengen we cannot access the immigration data, though we can the police data. How does that work practically, if all the information is on our national database that is on the central one?
Mr Thompson: The straightforward answer is that that is a level of operational knowledge I just do not have. If it would help, I am sure that I could ask Home Office colleagues to write in and give you a sense of that. I do not want to stray into areas about which I cannot say anything particularly knowledgeable.

Q123 ***Viscount Ullswater:*** Perhaps we should get down a little more to the specifics. SIS II proposals introduce the possibility of processing a new category of data, which is the biometric data. Do the provisions on biometric data provide sufficient protection for inaccuracy and misidentification following this one-to-many search, as highlighted by the EDPS opinion on the proposal? What is your view on that particular aspect?
Mr Thompson: Our view is that, in one sense, what we are waiting for here is the Commission report. Set out in the decision is an agreement that the Commission will come forward with a report which is an assessment on the reliability of the biometric technology, and indeed the state of readiness of the various Member States. That report itself will be subject to discussion in the Council and agreement by Council members, and also consultation with the European Parliament. I am not trying to duck your question at all. There is a sense in which we will get a chance to have a cold and rigorous look at those issues via that Commission report. It is envisaged, as I understand it, that biometric data will be very much used in conjunction with other data to verify. Used properly, one can see biometrics as a means of reducing misidentification. So, for example, in a large, EU-wide database, it must be quite possible that there will be people on that database with the same name. However, the idea that they will be on the database with the same name and, say, the same fingerprint, I imagine—and I am no expert in these matters—must be nil. I think that biometrics, properly used, can help with the quality of identification.

Q124 ***Viscount Ullswater:*** Surely that is the one-to-one search? To try and identify the person with the same name is a one-to-one search, whereas a one-to-many is when you flick the data into the huge database and see how many matches you might get. That is the one-to-many, is it not?
Mr Thompson: My understanding is that, certainly in the first instance, the one-to-one, as you call it—or the hit/no-hit—is very much what is envisaged for the SIS database. The Commission will be reporting on issues such as: is the technology there, and are the Member States in an efficient place where they can all sensibly and accurately add the data? However, this report will also discuss in detail the various problems associated with the kind of search you have been talking about. That is when Member States can take a decision, and come to a rigorous decision, about whether or not the sort of issue you are raising is adequately covered. I appreciate that I am slightly pushing my answer to a kind of "We'll know at a later

date", but I think that is the best guarantor we have here.

Q125 ***Lord Avebury:*** What you say is really alarming, because it will be possible for a law enforcement officer in a Member State to have a fingerprint, to enter that fingerprint into the system and to compare it with millions of other fingerprints. This is the kind of search which Viscount Ullswater has referred to, where error rates of up to two per cent have been found in other studies. Whatever the Commission may say, therefore, we are anxious—or, at least, I think that some of us are—about inaccurate false positives being thrown up by the system, and the degree of protection which is built in to safeguard against somebody being wrongfully accused or even arrested on the basis of the biometric comparison at that time.
Mr Thompson: I hope that I did not give that impression. What I was trying to suggest is that my understanding of this data based on the use of biometrics—and, again, Home Office colleagues may be able to be more knowledgeable on this than me—is that a decision has simply not yet been taken about whether to use biometric data in that way. A decision will not be taken until Member States have had the Commission's report, can air exactly the sorts of concerns you are raising, and feel satisfied on the accuracy of the data, that the safeguards are appropriate, and so on. We are not anywhere near that position yet. By simply agreeing the SIS II Decision, it does not automatically take us down that road.

Q126 ***Baroness Bonham-Carter of Yarnbury:*** Picking up on that, as regards the decisions on collection and storage of biometric data, are the Government concerned by the absence of harmonised provisions? What are the main points of conflict between data protection and the collection and use of the data?
Mr Thompson: The first part of my answer I will keep fairly brief, because there is a sense in which the answer to part of your question is again the Commission report—and that is something we will be looking at—and whether or not the Commission recommend harmonised provisions or, as may be more likely, minimum standards. One clearly needs to feel secure that, given that data is being inputted into the system from all Member States via these national databases, the quality of the data being put in is good. Also, one of the things that gives us comfort here is that there is an agreement in the decision that there will be special quality checks—I think that is the phrase used—which addresses that point too. On the conflict point, I do not think that the Government see it in terms of conflict, in the sense that data protection applies just as much to biometric data as it does to other kinds of data. So it is not that they are in conflict. What we want is an arrangement where we feel that the data protection rules which apply to biometric data give us the kind of comfort and security we want. It is not about conflict; it is about compliance here, I think.

Q127 ***Lord Avebury:*** Can you tell us about the question of transfer of data to non-EU states? The draft Data Protection Framework Decision allows that, whilst the SIS II Decision bars the transfer except to Interpol. Which rule will prevail if the Framework Decision is adopted? When you are answering that, can I also refer you to document 12924/06, which is a communication from the Council of the European Union to the Multidisciplinary Group on Organised Crime, in which they are saying that the adequacy proposals should be dropped from Articles 15.4 and 16, and it will be for each Member State to decide, where there is no bilateral treaty with a third state, whether the data protection of that state is adequate. We are therefore shooting at a moving target here, are we not? When we ask whether you think that the Data Protection Framework Decision should be the one that prevails, you have to make an assessment of which particular variant of the Data Protection Framework Decision will ultimately be adopted.
Mr Thompson: If it were that the Data Protection Framework Decision prevailed, that would be so; but my understanding is very much that SIS II rules apply in addition to DPFD rules and that SIS II rules, in the example you have cited, would prevail.
Ms Nowell-Smith: I could say a bit more about that, if you like. The way SIS II is drafted it provides higher standards of data protection because it is dealing with a very specific type of data, in a particular database. The DPFD covers all manner of data and is therefore a more flexible instrument. The relationship between the DPFD and SIS II is treated in two places in the draft texts. SIS II says that all data must be processed in accordance with Convention 108. The DPFD then says that in SIS II, wherever you have a reference to Convention 108—the 1981 Convention—all references to Convention 108 will be replaced by the DPFD. However, many of the rules in SIS II are not just based on Convention 108; the rule about sharing with Interpol, for example, is in addition to Convention 108. The time limits for keeping data—this three-year rule—are in addition to Convention 108. So while the DPFD will slot in, if you like, at the level of the Convention 108 protection, that would leave in place all the additional protections that are in SIS II.

Q128 ***Lord Avebury:*** Are you satisfied that the reference of all these questions about the Data Protection Framework Decision to the Multidisciplinary Group on Organised Crime is a

good way of dealing with the amendment of that document, and that it will not have any effect on the data protection system that applies to SIS II?
Ms Nowell-Smith: We are satisfied with that, partly because it is already expressed on the SIS II instrument the places in which the DPFD will come in to replace Convention 108. So the discussion about the level of protection that should be in SIS II, this higher level of protection, has already been had and is on the face of the SIS II document. No matter what the DPFD comes out with as a minimum standard, it will not be below Convention 108; it will be slotted in at that level and the specific protections will remain in place in SIS II.
Mr Thompson: From memory, the Council reached a common position on SIS II at the Justice and Home Affairs Council in October. The discussions within the Council have therefore finished. I think that the European Parliament vote on it this week. If they agree and there is a so-called "first reading deal", in effect the SIS II instrument is agreed.

Q129 ***Lord Corbett of Castle Vale:*** Can we just stay with Interpol for a moment, please? Will the Framework Decision be applied to evaluate whether Interpol and its members offer adequate protection to personal data?
Mr Thompson: The basic point I would want to make here, before going into some of the detail, is that no data will be shared by Interpol with a third country that does not have adequate data protection standards. They are not just going to spray it around to anyone. In addition, there is an agreement to be reached with Interpol, which from memory is Article 48AA and Annex 4, which sets out the basic principles of what an agreement with Interpol should be. I can quote it to you. These are quite tight requirements. "Ensure the security of the storage of transfer data"; "Mechanism for real-time update"; "Regulate the use of SIS II alerts by Interpol", et cetera. While that agreement has yet to be finalised, we are quite confident that SIS data that is shared by Interpol will be used properly. They are actually stricter rules and would take precedence over the rules that currently exist in the draft DPFD.

Q130 ***Earl Listowel:*** May I ask you about the access by security services? The Council's latest draft allows security agencies to have access to SIS II data and to input alerts concerning surveillance into SIS II. Is it acceptable that they will, as the latest draft provides, be exempt from the Data Protection Framework Decision?
Mr Thompson: The first thing I would say here is that anyone entering data or accessing data contained in SIS II will be bound by the requirements in the instrument. As to the DPFD, I am sorry, here I can be less forthcoming. That is because discussions are pretty live and this issue is a pretty live discussion. It is not at all clear yet in the Council working group, let alone when it goes to ministers, as to how the security service will be treated. I realise that is not a terribly useful answer, but I am not sure I can really go beyond that at this stage.

Q131 ***Earl of Caithness:*** I want to come back and spend a little more time looking at the difference between SIS II and the Data Protection Framework Decision, because that Decision allows sensitive data to be processed in certain cases whereas the SIS II Decision does not. Which rule will apply if the Framework Decision is adopted?
Mr Thompson: Pretty much the rule I mentioned before. As a general rule, SIS II rules prevail. In this case again, SIS II is adding additional data protection rules over and above what is in the DPFD. So in the particular case you cite, SIS II rules prevail.

Q132 ***Earl of Caithness:*** Are you happy that they should in this instance?
Mr Thompson: Yes, we think that is quite appropriate. SIS II is not a closed database, if you like, because data comes in and out; it is entered. However, it is a very specific database, used for defined purposes, and we think that the rules set out in the instrument as a whole are appropriate.

Q133 ***Earl of Caithness:*** If that is going to be the case, why is there such a difference between the Framework Decision and SIS II, if SIS II is going to end up ruling everything?
Mr Thompson: SIS II only works in relation to SIS II data. What the Framework Decision is trying to do is give a set of broad rules, if you like, right across the Third Pillar—which have been lacking. It is trying to bring general coherence and to stop Third Pillar instruments always reinventing the wheel in terms of data protection rules. It provides this minimum standard, this "floor" if you like, and the SIS II instrument—which, as I say, is quite a specific, contained database for a specific purposes—happens to have additional rules. I think that the difference is because they are trying to do different things. I do not know if there is anything you would want to add, Harriet, to illustrate that point?
Ms Nowell-Smith: The list of types of data that you can put into SIS II is defined in the instrument and it is very narrow. There is no need to put sensitive personal data in there. It is not relevant to any of the listed categories, and it should not be in the SIS II database. The Data Protection Framework Decision covers all data processed in the context of police and judicial co-operation. For example, information about a witness or a victim, if a victim has suffered physical injury due to an assault, that would be relevant data to be shared across borders in the

context of co-operation in the police or the judicial sphere. If a British person is harmed in France and the authorities want to share that data—it could be information about their religion, if it was a hate crime, or it could be information about their physical health—all that sensitive personal data is highly relevant to police and judicial co-operation and needs to be treated in the Data Protection Framework Decision, because obviously you need that kind of data for the purpose of police and judicial work.

Q134 ***Lord Avebury:*** Does not that raise a question in your minds that, if the rules in SIS II always trump the Data Protection Framework Decision with regard to SIS II, we are aiming at inadequate standards for the Third Pillar as a whole?
Mr Thompson: No, I do not think so. I think it is more a recognition of the fact, as Harriet has said, that because this is trying to provide an overview of the Third Pillar, and the range of data and the uses to which it would be put are so varied, it is inevitable that the Data Protection Framework Decision is a more—for want of a better word—subtle instrument: one that has to cope with more variation. It is just the nature of these two things. One is trying to provide a very general application; the other is a very specific instance.

Q135 ***Lord Dubs:*** Is that therefore your answer to my question as well? My question is about the time limits for storage of personal data. SIS II is quite precise; the Framework Decision is rather vague on this.
Mr Thompson: I am afraid this is where I get into broken-record territory. Yes, SIS II rules in this particular example do prevail.

Q136 ***Lord Dubs:*** I do not want to put words into your mouth, but you justify it by saying that the Framework Decision covers a wider range of things which are not so precise and do not need to be so precise?
Mr Thompson: It is not that they do not need to be so precise. I think that that level of precision in the wide range of cases that the DPFD covers is not practical. I think that is the distinction.

Q137 ***Lord Dubs:*** What you are saying applies to all personal data then, other than the bits covered by SIS II? I can see why in general terms there may be instances where the Framework Decision is appropriately wider or vaguer than SIS II, but I do not see why that should apply to something as clear-cut as time limits for storage of personal data. It seems to me that is a fundamental safeguard.
Mr Thompson: One of the reasons why time limits in the DPFD are longer than the three years in SIS II is for audit purposes. There are cases of people who have taken action where their data has been five years old, so there is a real point about audit in terms of data storage. Of course there must be a point at which time limits are very relevant, but the point is surely that the data is stored, treated properly, regardless of whether that data is kept for period-of-time "x" or period-of-time "y"?

Q138 ***Lord Dubs:*** May I move on? It seems to me that also there is a difference between the SIS II and the Data Protection Framework Decision as regards the further data processing that is permitted by the SIS II Decision. Will that prevail if the Framework Decision is adopted?
Mr Thompson: Again, in terms of further processing, in this case the SIS II rules apply to SIS II data.

Q139 ***Chairman:*** I am sorry, could you repeat that?
Mr Thompson: The SIS II rules prevail here again. They are the rules that apply to the SIS II data.

Q140 ***Lord Dubs:*** So what rule will prevail, if the Framework Decision is adopted, for the data that are not covered by SIS II?
Ms Nowell-Smith: The Framework Decision.
Mr Thompson:
Chairman: I think you have just shot Baroness Henig's—
Baroness Henig: I think I know the answer to my question! That is, the SIS II instrument will prevail wherever there are differences—
Lord Corbett of Castle Vale: You are giving the answer before we ask the question!

Q141 ***Baroness Henig:*** I will ask the question, because the SIS II Decision does not provide for a right to information, whereas the Framework Decision does. The Framework Decision allows for the blocking of data and marking of data, whereas the SIS II Decision does not. I am assuming—but you will tell me if I am wrong—that the SIS II instrument will prevail in these cases.
Mr Thompson: For once I can actually depart from this typescript! In fact, there is a right of information set out in the SIS II instrument, where the national legislation permits it. That right does exist in the UK, and it is Articles 50 and 52.
Baroness Henig: So this is an area of slight change.

Q142 ***Viscount Ullswater:*** Could I ask a supplementary? How does one exercise the right?
Mr Thompson: Off the top of my head, I am not quite sure.
Ms Nowell-Smith: In the UK, do you mean?

Q143 ***Viscount Ullswater:*** Yes, for the information held on SIS II. How do you exercise the right?

Ms Nowell-Smith: The data subject would write to the police body. The SIS II instrument has not yet come into force in UK law, so I do not know if there will be a central point of contact or if it will be diffused. The Home Office could, I am sure, tell you better than I could. However, the legal instrument provides that the access is in accordance with domestic law. The current position in domestic law under the Data Protection Act is that data subjects can ask data controllers and receive their subject access rights that way, and it is enforced by the Information Commissioner.

Q144 ***Lord Avebury:*** In the document to which I referred earlier, that is the document where the Council of the European Union asks the Multidisciplinary Group to consider certain changes in the Data Protection Framework Decision, there is a question about the deletion of Articles 19 and 20 of the original proposal, which imposes an obligation on Member States to ensure that data subjects would be informed of the fact that data was being processed about them. Are you saying that the deletion of these clauses is happening and that they will be replaced by an article which leaves this to the legislation in individual Member States?
Mr Thompson: Perhaps I could ask Harriet to take that question, if only because she is much closer to the detail of the DPFD negotiations than I am. I think that she could give you a fuller answer.
Ms Nowell-Smith: Again, there is not too much we can say about the current state of the negotiations, because they are regarded as confidential by the Commission and the position of other Member States is something that I cannot really comment on. The UK's position is that we provide access rights to data subjects in this area under domestic law. We are content for it to happen in the Data Protection Framework Decision. You might also like to note that the articles you referred to distinguish between data that is collected from data subjects and data that is collected from third parties, which is an important distinction to keep in mind in those sections. The basic principle that there should be a right of access in Article 21 of the Data Protection Framework Decision I believe is not referred to in that communication. I do not have it with me today.

Q145 ***Lord Avebury:*** That is correct.
Ms Nowell-Smith: It is the provision that provides right of access to data that is held about people. The articles you are discussing, Articles 19 and 20, are about the different circumstances in which the police, for example, have to notify people that they do hold data. Sometimes it is obvious that the police hold your data. If you have been interviewed by someone in uniform at a crime scene, you will know that they have your data. Sometimes, if there is a covert surveillance going on, hopefully you will not know that the police have your data! So the notification rules are complicated, but the basic right of access, to be able to ask the police whether or not they have your data and to show it to you, is something that is in Article 21, and I believe that is not in question in the communication to which you have referred.
Lord Avebury: That is very helpful.

Q146 ***Chairman:*** I should have said earlier that you will be sent a transcript of this meeting in due course. When you look at the transcript, not only to make sure that you are correctly recorded but if it occurs to you that there are things that you should follow up in writing to us, that would be very welcome.
Mr Thompson: Of course, yes. We will try and do that as quickly as possible, because I know that you are making good progress on this.

Q147 ***Lord Dubs:*** The SIS II Decision and the Framework Decision both emphasise the importance of judicial remedies as regards data protection. At present, British courts cannot make references to the Court of Justice under Third Pillar matters because the Government have not opted in to the Court's jurisdiction. Is that something the Government are planning to reconsider?
Mr Thompson: You will appreciate this is a government position beyond the sole responsibilities of the Department for Constitutional Affairs, but it is certainly true that the Government keep under constant review this question about EC jurisdiction and the Third Pillar. At the moment, we have no plans to change our current position. From memory, there are 14 Member States who have decided to come under the jurisdiction of the ECJ and the Third Pillar. We are not one of them. From memory, I think it is Ireland, Denmark, and probably the eight accession countries comprise the others.

Q148 ***Lord Corbett of Castle Vale:*** Are the Government content with the progress of negotiations on the Data Protection Framework Decision?
Mr Thompson: We have always supported rapid progress on the DPFD. From memory, it came out at the tail end of our presidency; so we were not able to do much with it. We supported progress during the Austrian presidency, and we have certainly supported the efforts that the current Finnish presidency has made to up the pace on negotiations. My understanding is that the Finnish presidency hopes to conclude the DPFD by December of this year. If that is not possible, we would hope that the German presidency, which follows them, would similarly give this priority.

Q149 ***Lord Avebury:*** I am wondering whether you can say anything about the legal status of the Multidisciplinary Group on Organised Crime. What was the legislative instrument under which it was set up? Is it really satisfactory that the Council should delegate responsibility for progress on the DPFD to a body whose members are anonymous and where we do not know if it contains any experts on data protection?
Mr Thompson: On the first point, I am afraid that offhand I do not know its legal basis. It is very much a Home Office lead. My understanding is that the Multidisciplinary Group is merely throwing its comments into the ring, if you like. The main body conducting discussions on the DPFD is the Council working group, with representatives from all the Member States, and that is the body of which we, the Department for Constitutional Affairs—who, after all, are responsible for data protection in the UK—meet with our colleagues, our opposite numbers, and that is where the main negotiations take place. I do not know if you have anything to add, Harriet?
Ms Nowell-Smith: We do attend the MDG. I do not know the legal basis on which it was set up.
Mr Thompson: If it is helpful, we can either speak to the Home Office or ourselves write back to you and clear that up.
Chairman: That would be very helpful.

Q150 ***Lord Avebury:*** Do you know whether it contains any experts on data protection?
Ms Nowell-Smith: I feel I can assure you that it does. The UK delegation is represented by the Department for Constitutional Affairs, so we are the ones who attend these working groups. That is because it is primarily a data protection instrument. Many countries also send data protection experts. If they send crime experts, they are crime experts with an expertise in data protection, as far as I am aware.
Mr Thompson: Can I record that I have made a mistake there? It slipped my mind that in this particular case the Council working group I referred to is of course the Multidisciplinary Working Group. That is confusion on my part, and I would like to correct that for the record, if possible.

Q151 ***Lord Corbett of Castle Vale:*** Would the adoption of the SIS II Decision or the Framework Decision entail any amendments to the UK's national data protection laws?
Mr Thompson: Implementation of SIS II is for the Home Office. I know that they are considering this matter at the moment, although they have not reached a decision. My understanding is they are looking for a solution which is practical; something one can do quickly and which is, clearly, legal. I just do not know beyond that.

Q152 ***Earl Listowel:*** If I may, I would like to ask a question about the Schengen evaluation team. This came up in our first evidence from the Home Office. I think that there is some scepticism about the effectiveness of that team. Can you reassure us that this is in fact well resourced? That, for instance, if it has concerns about new accession countries, they have the resources to address them? Do they report back? Is there clarity to the public about those reports?
Mr Thompson: I do not think there is much I can add, in the sense that I have not heard any concerns that they are either under-resourced or not doing a proper job. You are right that there is this Schengen evaluation team, made up of representatives from Member States. Before anyone can join the Schengen Information System, they make an assessment as to whether or not that particular Member State's systems are sufficiently good. I have not heard any concerns, but I cannot really go beyond that.

Q153 ***Earl of Caithness:*** May I ask a question about how some of this will work in practice? What are the implications for our police and judicial services when they are collecting data, when they have to determine whether it will be used solely within the UK, or whether it will be used within the Framework Decision, or whether it will be used within SIS II and hawked round the EU and other countries outside? How will poor Mr Policeman, when he collects the data, determine that and the way in which he takes the data? Because the way he collects it and the way he handles it will have implications, depending where it finally ends up.
Mr Thompson: I am not sure there is anything by way of real detail I can say that is useful here. Our department's interests are in the appropriate data protection rules that apply to the database as a whole. What we do not have responsibility for is how we implement it and how the police will. I just do not have that kind of information at hand. What I do know is that the main components of SIS data, for example, will tend to be people who are wanted for some reason. An obvious example might be that there is a European arrest warrant against them. That would be an obvious trigger as to why you would put something on SIS. People who are missing and people who are under surveillance—my understanding is that is very much the bulk of people who might actually be on SIS. I do not know whether there is any extra detail you are aware of, Harriet?
Ms Nowell-Smith: It is easier to think of it in a staged way. Therefore, when you are collecting detail and you are a policeman just doing your normal job, you would be applying the Data Protection Act already. When you decide to enter information on to SIS II, at that point you have to think about the rules in SIS II. Most of the rules in SIS II, though, would be

about the length of time for which you keep data. That kind of rule I would not expect to be applied by each policeman putting data into SIS II. It would be managed by the national body that maintains the database. So that part you would address only when you were entering information on to SIS II. We do provide a high level of data protection in the police and judicial areas already, so there is less risk for the UK than for some other Member States of having divergent levels of data protection for different types of data. Obviously we want a simple system that everyone can understand and work with.

Q154 ***Chairman:*** Thank you both very much indeed. You have been very helpful and we are most grateful to you for answering as you did. I remind you that we would very much welcome any subsequent written comments, if you think that those are required when you look at the transcript. I think that now, in a seamless way, we will change witnesses. You are both very welcome to stay if you want to.

Mr Thompson: Thank you very much. Once we have seen the transcript, we will certainly bear in mind whether or not we need to get back to you and clarify matters.

Memorandum by the Information Commissioner, Richard Thomas

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this evidence are primarily from the data protection perspective.

2. The Commissioner has been provided with powers to enable him to perform the role of the United Kingdom's data protection supervisory authority as envisaged by Article 114 of the existing Schengen Convention. These powers will enable the Commissioner to assess whether personal data recorded in the Schengen Information System is processed in compliance with the Data Protection Act 1998. These powers are set out in section 54A of the Data Protection Act 1998 (amended by virtue of the section 81 of the Crime (International Co-operation) Act 2003).

3. Although the United Kingdom has yet to participate in the Schengen Information System, the Commissioner has been invited to participate as an observer in meetings of the data protection Joint Supervisory Authority established under Article 115 the Schengen Convention. This has allowed him to participate in discussions on the data protection issues arising from the move to SIS II.

4. The Joint Supervisory Authority has produced a detailed opinion on SIS II, including a commentary on the various articles of both components of the proposed legislative basis for SIS II, the proposed Regulation (COM (2005) 236 final) and the proposed Decision (COM (2005) 230 final). The Schengen Joint Supervisory Authority has many years of practical expertise of the current arrangements including conducting compliance inspections. It is particularly well placed to provide an authoritative view on the likely data protection concerns arising from the proposals to introduce SIS II. The Commissioner was able to contribute to discussion whilst the Joint Supervisory Authority was drawing up its opinion and he endorses the comments made in it. A copy of the opinion is attached.

5. The Joint Supervisory Authority opinion is a detailed document and given the Commissioner's support for its observations it is unnecessary duplication to reiterate each of these separately. In view of the detailed nature of many of the observations it is worth highlighting the main areas of concern:

— The application of current EU data protection laws allied with the present proposals will result in four separate EU legal instruments applying to SIS II. This produces a confusing picture and it is in the interests of all if the legal basis is clear and comprehensive.

— It is not clear who will be responsible for SIS II as some responsibilities fall to the Commission, others to the Member States. There is no clear designation of who is the data controller and the legal basis should make this clear.

— The purpose for SIS II incorporates the specific purpose of conducting entry controls with more general purposes of assisting police and judicial cooperation. The specific inclusion of Europol, Eurojust and vehicle registration authorities highlights the increased move to the use of SIS II as an investigation tool. Clarity of purpose for the processing of information is essential.

— The proposed data protection supervision arrangements could lead to a weakening of protection. The current arrangements for central supervision by a joint Supervisory Authority comprising the national supervisory authorities is replaced by divided responsibilities between the European Data Protection Supervisor (for the activities of the Commission) and national supervisory authorities for the processing of personal data on or from their territories. The new arrangements place too much emphasis on monitoring of central processing which will be minimal and there is a need for an institutionalised role for cooperation between national supervisory authorities akin to the current Joint Supervisory Body arrangements.

6. The Commissioner would also draw the Sub Committee's attention to the Opinion of the European Data Protection Supervisor on the proposals for SIS II. His opinion is of particular relevance given his role in monitoring the activities of the Commission. This opinion is attached for information.

7. The Commissioner is concerned about the proposed data protection supervision arrangements. Experience gained in his participation in the work of the joint supervisory bodies for Europol and Customs Information System together with that of the Schengen Information System all points towards the need for very close cooperation when international information sharing systems are established. It is vitally important that all the national supervisory authorities act together with a common commitment and understanding when undertaking work such as compliance auditing. Being able to decide common approaches with colleagues and put these into practice has proved an essential feature of a relatively seamless and consistent form of data protection supervision across national boundaries. The opportunity to discuss problems together and arrive at common agreed solutions has proved most useful. Whilst some reduction in the bureaucracy accompanying the current arrangements would be welcome preserving an effective forum for discussion and coordinated action is essential. Whilst the proposed arrangements do envisage an element of cooperation and liaison between the EDPS and national supervisory authorities this does not provide for the same level of cooperation as currently enjoyed. Undoubtedly there would be great will between the parties to make the arrangements work in practice but the lack of a forum for national supervisory authorities to decide on matters and take action collectively both centrally and at national level is a practical concern.

8. The use of different legal instruments in the proposed Regulation and the proposed Decision as the basis for providing effective data protection safeguards undermines the need to adopt a consistent approach founded on equivalent standards. In the proposed Regulation it is primarily the Data Protection Directive (95/46/EC) whilst in the proposed Decision it is primarily the Council of Europe Convention 108. This difference once again highlights the need for an EU data protection framework for Third Pillar matters. The Commissioner has previously given evidence to the Sub Committee on the desirability of establishing a Third Pillar data protection instrument as part of its inquiry into EU Counter Terrorist Activities. The varying legal standards that are being deployed for the commencement of SIS II provide a good example of the pressing need for prompt adoption of such an instrument.

9. To be able to undertake effective supervision it is necessary for a data protection supervisory body to have full access to the personal data held. Article 114.1 of the current Convention provides for a national supervisory authority to have access the data file in the national section of the SIS. The proposals at Article 52 (proposed Decision) and Article 31(proposed Regulation) merely require that the national supervisory authority monitors the lawfulness of the processing. There is no specific reference to the extent of information available to it to achieve this objective and this ambiguity should be resolved to ensure that full access to data is available.

10. As stated above the Commissioner's powers to undertake functions in relation to the Schengen Information System (including any replacement system) are governed by section 54A of the Data Protection Act 1998. This section provides for the Commissioner to inspect any personal data recorded in the Schengen Information System at national level. Given the concerns expressed in paragraph 9, it is important that this level of supervision is not subsequently weakened by adoption of ambiguous wording in the two instruments. A further example of the ambiguity caused by the approach is apparent when comparing the provisions relating to the powers and duties of national supervisory authorities. In the proposed Decision, Article 53 provides specific powers for independent monitoring. The proposed Regulation adopts a slightly different approach by referring to these by reference to the powers conferred upon such authorities by virtue of Article 28 of the Data Protection Directive 95/46/EC. It would be undesirable if such a reference was seen as limiting supervision powers in any way.

11. An important feature of both the proposed Decision and Regulation is the communication of information to the public by way of an information campaign. Article 14AA (proposed Decision) requires the Commission in cooperation with national supervisory authorities and EDPS to launch an information campaign to

accompany the start of SIS II and repeat campaigns regularly. Whilst such a campaign would be desirable, the extent of the involvement of national supervisory authorities and the financial resources this would involve is not clear. It is important that at national level the requirements on Member States to ensure that their national supervisory authorities are provided with the necessary resources for their tasks take account of such a potentially significant financial commitment.

12. The Commissioner hopes that the evidence provided to the Sub Committee assists in the consideration of this important matter and he is happy to assist it further if required.

12 July 2006

Examination of Witnesses

Witnesses: MR DAVID SMITH, Deputy Information Commissioner, and MR JONATHAN BAMFORD, Assistant Commissioner, Information Commission, gave evidence.

Q155 ***Chairman:*** You are both very welcome. I think I am right in saying that we welcome both of you back, do we not? You have both appeared before this Committee before?
Mr Smith: Yes.
Mr Bamford: Yes.

Q156 ***Chairman:*** Thank you very much for coming. We will perhaps start by asking you if you have any comments on the previous session. Is there anything touching on your responsibilities that you think we ought to know about? Perhaps most particularly on the last question, which was whether the adoption of the SIS II Decision or the Framework Decision entailed any amendments to the UK's national data protection law. From your point of view, what is the answer to that?
Mr Smith: Thank you, My Lord Chairman. If you do not mind, may I also say a word or two of introduction?

Q157 ***Chairman:*** Please do.
Mr Smith: I have been here before, as you know, and it is a pleasure to come back again. My colleague Jonathan Bamford takes charge of these areas for us. I am now Deputy Commissioner and essentially have responsibility for all our data protection functions in the Information Commissioner's Office. Mr Thomas, the Commissioner, does send his apologies for not being able to attend today in person. As I say, we welcome the opportunity to come here. We really do appreciate the interest this Committee shows in Third Pillar data protection issues. It is an important area for us, but is often one on which little light is cast. We have a particular interest in Europol, which is what we have spoken to you about before. I do not want to blow my own trumpet, but you may be interested to know that I was elected last week as Chairman of the Europol Joint Supervisory Body. It is not a personal thing, but I think that it is a mark of the UK's interest and engagement with those issues.

Q158 ***Chairman:*** Congratulations personally to you!
Mr Smith: Thank you, My Lord Chairman. Having said that, it is perhaps more a word of apology to you that our involvement with SIS, and particularly SIS II, is less than that with some of the other areas. We are only observers on the Joint Supervisory Authority at the moment; we have no practical experience because SIS is not operational in the UK. In coming to you today, therefore, we are more than happy to come and give evidence but, if we are a little hesitant on some points and say that we need to go back, think about it and get back to you, please bear with us.

Q159 ***Chairman:*** I understand that. May I just ask this? Does your observer status in fact limit the extent to which you can intervene and influence the negotiations?
Mr Smith: No, it does not. We are able to speak in the meetings. We do not simply sit and listen; but I think that we are a little reluctant to, if you like, keep putting up our hand and to keep getting involved when we are not there as full members and certainly, on the odd occasion that issues come to a vote, we do not have a vote on those issues. You asked about the changes in the Data Protection Act required by SIS II and by the Framework Decision. I am not sure that the SIS II alone would require changes in the Data Protection Act. My assumption is that there will be some implementing legislation which would translate the provisions into UK law. We come back to this question which you were asking about. Which prevails? The general data protection or the specific legislation? And I will happily deal with that. I think that the implementation of the Framework Decision would require some changes to the UK Data Protection Act. It is very unclear to us at the moment how that Framework Decision will emerge. We are pleased by the interest you have shown in that in the discussions and we are happy to answer some questions on it, because I think that we do have real concerns, from the limited feedback we get, as to

where the negotiations which have been referred to are actually leading.

Q160 ***Chairman:*** I should have said earlier that we are very grateful to you for the written evidence which we received from you. It is very helpful. Perhaps I could widen the question of legislation slightly, to ask you whether your Office is concerned about overlaps between SIS II texts and different EU and EC data protection legislation. In other words, we are moving wider than British legislation to EU. Are you able to give us an answer to that?
Mr Smith: The very simple answer, My Lord Chairman, is yes, we are concerned. We are particularly keen in the Information Commissioner's Office at the moment to comply with better regulatory standards, making the law clear and accessible. I have to say that what we see here in this area goes completely against that, because there is such a myriad of legal instruments. In the First Pillar area we have the regulation and, at Member State level, the Data Protection Directive 95/46/EC will apply, and national law will flow from that. In the Third Pillar area we have the decision and Convention 108 of the Council of Europe, coupled with the recommendation on police data, which may be replaced by the Framework Decision and then that translated into national law. So far as the central processing is concerned we have the Council Regulation 45/2001, setting up the European Data Protection Supervisor. So it is an extremely mixed picture. We have difficulty following it. The public, who are the ones who are important—individuals whose data may appear in the system—we feel will have real difficulties exercising their rights. In the earlier evidence you referred to judicial remedies and going to court. What will the court make of this? We talk in our Office about judicial remedies, and we think of the person who is going off perhaps to Bolton County Court to get their remedies.

Q161 ***Chairman:*** Perhaps we should ask the next question of the courts rather than of you! If there is a conflict between SIS II legislation, the Framework Decision and national data protection legislation, which should prevail? Or are we simply looking for the higher standard of data protection?
Mr Smith: I think that you are looking for the higher standard, although I am not sure that it is really a question of one prevailing over the other. It is the sort of situation I was discussing with my colleague earlier, which we have all the time in the UK anyway. We have national data protection law here; we now have legislation on identity cards. There are some specific measures in the identity cards legislation which set out data that will be held in the system, and they set out ways in which security will apply. So this specialises, if you like, some of the data protection measures. I think that, in his opinion, the European Data Protection Supervisor talks about *lex generalis* and *lex specialis*. I hesitate to go too far down that route, but I think that he gives a good description. One is the general law which applies when nothing more specific exists in the Schengen legislation but, if there is something more specific in the Schengen legislation, that takes over. An example would be fingerprint data. You might be able to argue, whether under the general Framework Decision or the UK's general data protection law, that fingerprint data is excessive; that it breaches the requirement that data should be not excessive. However, I think it is very hard to pursue that argument if the Schengen legislation says that fingerprint data will be an item in the system; if the legislature has decided that. On the other hand, the Schengen Decision is more specific in areas like audit trail requirements. The Framework Decision and our data protection law require adequate security and it goes into a little more detail about what that means; but the Schengen Decision talks very specifically about the audit trail of information which will be kept, who will have access to it and how long it should be kept. That is how we see it, but it is a difficult picture that we are left with.

Q162 ***Lord Avebury:*** You heard the argument that was being put to us by the DCA that there was a difference between the specific needs of SIS II and the much wider area of data to which the DPFD would apply, and that this justified the existence of two different instruments. Were you satisfied that there was that logical reason for the distinction? Also, that the assurances they gave, that wherever SIS II provided a superior degree of data protection it would trump the DPFD but, on the one example where the DPFD provided superior protection, it would trump SIS II, was that a reassurance that was valuable and satisfactory?
Mr Smith: In simple terms, yes, it does provide some reassurance and it is how we see the picture—this *lex specialis* and *lex generalis*. However, the underlying level of data protection, both in the Schengen system—where there is nothing more specific—and more generally across the Third Pillar, will be the Framework Decision. I would say that we would be more reassured were we confident that the outcome of discussions on the Framework Decision would lead to a data protection instrument which was at least as good in terms of rights of individuals and protection as that which currently exists in the First Pillar, through the Data Protection Directive.

Q163 ***Earl of Caithness:*** I was concerned by an answer you gave to Lord Wright earlier, when you said that you were concerned that only limited information was available to you. Who is not giving you the information?

Mr Smith: My colleague can perhaps say a little more. I think that when Harriet Nowell-Smith gave evidence she touched on the issue. I would want to be very clear with you that the Minister, Baroness Ashton, has given assurances to the Commissioner in that she wants us to be fully involved in negotiations and discussions on the Framework Decision. The difficulty is, when that is translated down to official level, it does not always come through, and part of it is this confidentiality which surrounds the negotiations. We are to some extent excluded because of that confidentiality. I think there is an argument that we should be a trusted expert party and within the bounds of that discussion—in the way that, as we understand it, some of our European colleagues are. Sometimes we find out more through other data protection authorities than we find out through government departments.

Q164 ***Chairman:*** Are your European colleagues also suffering from this a bit?
Mr Smith: Yes, I think that is fair. It is not unique to here, but we feel that there is—not just in the UK, no, but also at the European level—a lack of expert data protection input into these negotiations which have been referred to.
Mr Bamford: When we talk to our European colleagues it is a variable picture. Some seem much better informed, always seem to have the latest version of every text available and are happy to share that, than others. We probably feel ourselves to be slightly in the other category on that one. That is not because we have not had contact with the DCA. We were involved in the stakeholder consultation which they did on the Data Protection Framework Decision. To put it into context, however, as part of that we were there with civil society organisations and were placed under restrictions to hand texts back and not to keep them. As David has said, perhaps we enjoy a different sort of relationship and have a different sort of expertise there, enabling us to be more actively involved in the process than in the twists and turns of the way the negotiations go on the Framework Decision, and being able to have some input there. That has not always been possible in the past.

Q165 ***Chairman:*** This is rather beyond the scope of this meeting but are the rules of procedure for your European colleagues, if I can again use that expression, very similar? Are they identical and is their status vis-à-vis their governments identical to yours?
Mr Bamford: I think in other jurisdictions there is much more of a concept that the opinion of the supervisory authority, the National Data Protection Authority, has to be sought as part of the process of new legislation and new initiatives. It is not the case in the UK that there is an onus to do that. Often we are fortunate and the virtuous activities of government departments mean that we are involved in the process in some way but it is not the case as it is in other jurisdictions. We see there is a difference between where departments of state feel they have to consult with their National Data Protection Authority and ourselves where it is something which is nice to do, if I can put it that way, rather than actual requirements. To put it simply, we feel that we are one step behind some of your international colleagues in where we are up to and I do not believe that is as a result of any wish to exclude us from the process, perhaps some of it is the practicalities. One of the rules, as I understand it, is that only arms of Government can have the latest versions of the Framework Decision that is being negotiated. Clearly, we are not an arm of Government any more than the police are an arm of Government but do we get treated in the same way as other people like SOCA and others? If they had to give the text back as we do, that is fair enough but we want to be treated on all fours with those sorts of bodies that have a real direct interest in this.

Q166 ***Baroness Bonham-Carter of Yarnbury:*** You said in your written evidence to us that it is not clear who will be responsible for SIS II as some responsibilities fall to the Commission and others to the Member States. Are you still concerned about the lack of clarity as to who will be responsible for the management of SIS II?
Mr Smith: We still have some concerns and I would not want to overplay them. Our concern is to identify who is the data controller in our terms which is the organisation that controls the purposes and the means of processing in the system. We still have some doubts as to what operational management means, whether it is for the Commission or this management authority which is proposed. The way we see it, although it is not defined in the text and it would be helpful if it was, is that the management authority or the Commission will be a data controller and an organisation in each Member State, like SOCA in the UK, will be a data controller. You have a system of joint data controllers and joint responsibility which is fairly common place, particularly with shared information systems. What we always recommend domestically is that where you have those shared responsibilities, you have some sort of laying down of where the boundaries lie and who is responsible for what. It is not that everybody is responsible for everything. Naturally here the responsibility for the accuracy of the data rests with the data controller in the Member State. The management authority is unlikely to have any control over the actual information but some of the security arrangements are clearly with the management authority. You can

work out a lot of it but we would like to see it clearly defined so that essentially everybody knows what their job is.

Q167 ***Baroness Bonham-Carter of Yarnbury:*** We did hear some concern expressed last week about this management authority and the idea that it would be better if it was the Commission running SIS II was expressed. Do you share that view or are you less categorical?
Mr Smith: We would be less categorical. As a natural reaction, without hearing arguments why people think it should be the Commission, I hesitate a little. I think our view is that, in general, in applying data protection provisions we are not stuck on who it is who exercises functions so long as they are subject to the right controls. Our concern would be if in going to the management authority somehow the rules were slackened, the level of supervision was somehow less, that would bother us, but we do not see that necessarily follows.

Q168 ***Lord Corbett of Castle Vale:*** Do you feel that the agreed text which we were talking about in the last question provides for sufficient clarity and appropriate limits as regards the purposes of the processing of information?
Mr Smith: I suppose, in summary, it is better than it was if you will forgive me and I am happy to elaborate on that. I suppose what we have never had clearly explained to us, and I do not know whether anybody has explained it to your Committee, is just how the new system will be used and how the way in which it will be used will be different from the way in which the current system is used which is essentially as a hit/no hit system. Our simple take on the existing system is that you have to have someone there who you have arrested, you have stopped at the border or whatever and you do a check against the system on that person, "is there a hit?" We can see that having a fingerprint—someone will not give you their right name or whatever—is helpful to that process. Some of the things in the decision and some of the things that have been added help confirm that is still how it will be used. I think the words "compensatory measure" have been added in in Recital 5 which suggests it is still compensation for the removal of border controls which is a limiting factor. Article 40 talks about the data in each category of alert only being processed for the purposes for which it was put into the system which is encouraging in itself. Then Article 40(4) talks about some exceptions to that including, where necessary, for serious offences and views on what is a serious offence differ widely around Europe, maybe even within Member States. Some further definition there would help limit what is going on here. Having said that, it does talk about "it can only be used for those further purposes with the agreement of the Member State that put the data in" so that is a compensating measure. I think one area we would like to highlight is the one you referred to in the earlier evidence with the DCA, fingerprint data. I think it is Article 14 which says that fingerprint data can only be used to verify the identity of somebody, so you have got someone there and you use the fingerprint to check. This is not a problem. It is the possible extension in the future to essentially enable fingerprints to be run against the Schengen System. It does seem to us there is a possibility of a fingerprint being found at a scene of crime in the UK and not only do you run that against the UK fingerprint record, you run it against the Schengen System to see if there is anything that matches. This is becoming an investigative tool, not a replacement for removal of border controls and some of the things like access by Europol also feed into that. Europol is very much an analytical intelligence investigative type of organisation, so how will they use their access? We have this underlying concern of function creep, I think we have used that term here before. There is scope for function creep here and we are concerned that there may be inadequate control over that.

Q169 ***Viscount Ullswater:*** How possibly then can you control function creep because if the information is shared from a national database to the Schengen information service database, that database is going to be shared with Interpol, it is exactly the description that you have made which is likely to happen. If data held on a national database arrives at Interpol, then if there is somebody who has committed a crime, is it not likely that could be the route where this fishing expedition could occur? You have got these massive databases which are perhaps inter-operable, I am not sure. It would be very useful for Interpol to be able to access all of that fingerprint evidence which is provided by all the Member States through Schengen.
Mr Smith: I think there is no basic problem with Interpol having access on the same terms as the intention of the system, this checking an individual who has given a fingerprint. The danger is if you transfer the data to Interpol, are there any rules within Interpol or are there any obligations imposed on Interpol through an agreement which limits them in how they use it and, if there are, are you confident that Interpol will follow those? I think the answer may well be yes for Interpol, but Interpol is just an example of many possible transfers outside the European Union.

Q170 ***Chairman:*** Your new position to which you have just been elected, does this give you a closer relationship with Interpol as well?

Mr Smith: No, not directly, it is with Europol. There is a Europol/Interpol agreement on the exchange.

Q171 ***Chairman:*** There is a Europol person in Lyon, is there not?
Mr Smith: That is right, yes. My colleague has been to Interpol, I have not yet been there. One thing which does concern us slightly is to do with transfer to Interpol. The decision talks about an agreement with Interpol on the adequacy of the level of protection of personal data provided to Interpol of which we are fully supportive. It talks about the Council seeking the opinion of the Commission on the adequacy of the level of data protection at Interpol. It makes no reference to seeking an opinion of a data protection authority. In the first pillar the Commission makes decisions on the adequacy of third countries but it does so after seeking the advice of the Article 29 working party of the Data Protection Commissioners. With Europol, I think it is the management board that makes decisions on the adequacy of third countries for transfer but after seeking the opinion of the joint supervisory body. There does not appear to be any mechanism in this arrangement for those sorts of views to be sought.

Q172 ***Lord Avebury:*** I was going to ask you on the adequacy, and we have already put this to the DCA witnesses, whether amongst the requests for an opinion made by the Council to the MDG, one would ask them to consider the deletion of the adequacy provisions had you got the transfer of data to third countries in Articles 15(4) and 16. Do you know whether that extends to transfers to Europol and Interpol and have you any input with the MDG so that you can influence the way that this discussion goes?
Mr Smith: The issue you raise is one which, if you like, we have heard. What we received—the latest news we had—was at a meeting of the Police Working Party of the European Data Protection Commissioners where we were given a report last week about how the negotiations are going in the multi-disciplinary group which use words like "disappointing, lack of data protection expertise, questioning basic data protection principles which are well established including those on the adequacy of transfer to third countries". We are concerned that with some of the things which we see as fundamental to international instruments on data protection, like adequacy of transfers, like Articles 19 and 20 that the DCA witnesses referred to on the provision of information, there is talk of taking these out and simply removing them altogether which we find deeply worrying.

Q173 ***Lord Avebury:*** You do not have sight of the memoranda that were produced by the MDGs?
Mr Smith: No.

Q174 ***Lord Avebury:*** Can I go on to ask you with regard to the provisions and the agreed text for supervision of data protection at national level, and you have already described what the arrangements are within the United Kingdom, do you think the texts are sufficiently prescriptive as regards the whole of the European Union to ensure that the arrangements in other EU countries are as sufficiently robust as ours are?
Mr Smith: I think that is hard to say. Most European Member States have done the same as the UK and applied data protection law based on the first pillar instrument, the Data Protection Directive 95/46/EC. When they have applied it domestically, they have applied it across the board even to third pillar activities and that does provide a good basic level of data protection, so I think in practice there is a limited problem but there is scope for difficulty even in the UK. I have heard no suggestion that it will happen but the Data Protection Act that we have could be repealed in respect of the third pillar and our worry is that we do not have anything at European level to underpin it There is nothing at the moment other than the Council of Europe Convention 108. I think it is hard to see how the Framework Decision could have any provisions less than Convention 108 because this is part of the terms of the European Union so at least it will come up to that level, but it may not be much better than that. In practice this may not be a problem in most Member States but it does leave a gap in what underpins the arrangements which would be worrying.

Q175 ***Viscount Ullswater:*** Is the Information Commissioner's office still concerned that the SIS II decision will not require Member States to confer sufficient control powers on the national data protection authorities and would the proposed Framework Decision on data protection solve this issue sufficiently?
Mr Smith: We still have some concerns in this area. It is one of the things where we come back to, if you like, the complicated nature of the legislation surrounding this area. The existing Schengen Convention, I think it is section 114, talks about the powers of supervisory authorities and it says very clearly, " . . . shall have a power to inspect or access the data in the national section of SIS". As far as we can see, that is not as clearly replicated in the new decision. There are some measures there which give us some reassurance. There is something, I think it is Article 11, which says that we have to be given access to the audit trail but not necessarily to the data. There is a provision in Article 53 about conducting audits at least once every four years and there is a very genuine question of how could we conduct an audit if we were

not given the power to go in and look at the data. In the UK we have been given a power to inspect the national section of the Schengen System and we find it hard to believe that would suddenly be taken away from us. Again, is there really this underpinning? I think what has always been an issue for us with our powers, is that the existing power we have is to inspect the data in the national copy of the Schengen System so you just look at what is there. What is important to us very often is how the data got there. If there was an alert on me in the system, it does not help the supervision very much just to be able to go and look and see that there is an alert under Article 96 or whatever under the current arrangements without going back to trace in police systems here how it got there, when was I arrested or whatever, what was recorded in the police system, where was the decision that it was appropriate for this to be put in the Schengen System? We do not have—and there is nothing in this arrangement which gives us—an assurance or a power to go and make those sorts of checks. It also limits our ability to co-operate with other data protection authorities because there has been a very welcome move, and the JSA has initiated this, in doing co-ordinated checks, first on Article 96 data and more recently on Article 99 data where each Member State looks at what is in the system and traces it back and comparisons are done. There is a danger we will be cut off short and not be able to make the same contribution to that because of our limited powers. It is of concern to us. I have to say it is not confined to Schengen issues but it is here that it is heightened.

Q176 ***Chairman:*** Are the existing powers for information authorities like ourselves in the European Union fairly consistent or are you conscious of some of your colleagues having much more power—or less—than you do?
Mr Smith: Some of our colleagues have powers that we could only dream about! The Spanish data protection authority has powers to impose administrative penalties, I think they are, of many hundreds of thousands of euros, the result of which they keep for their own authority to help their function.

Q177 ***Chairman:*** We should send a copy of this transcript to the Treasury!
Mr Smith: That is right. We are not in any way suggesting those powers are necessarily right or appropriate for us. The powers do vary hugely because the legal framework and the whole approach vary hugely; in some areas we have better powers. There are criminal offences under UK data protection law, particularly for unlawfully obtaining or disclosing data. You may know we recently published a report, *What Price Privacy?*, calling for the penalties to be increased to prison sentences. I am happy to place on record that we are very encouraged by the government response to that and they have gone out to consultation on increasing penalties to prison sentences. That is something that many of our colleagues in other Member States would be in some way jealous of, but I think the area where we appear to have much less power is in the power to go in and make checks without the consent of the organisation.

Q178 ***Earl of Listowel:*** In evidence we have received it has been pointed out the records of information kept by the authorities might be improved to enable better auditing and observing how much added value that provides. For instance, the authorities which obtained access to SIS II, the nationalities of persons stored in SIS II, the decisions or measures which had been taken on the best basis of SIS II information, would you like to see that improved detail of information kept? Would it be, do you think, maybe too heavy a burden to move that far forward?
Mr Smith: I think it would be helpful for there to be some record-keeping. Were we able to make the sort of checks that we are talking about, it would be very important to be able to see why the data was put in the system, who took the decision and when. Having said that, we are very conscious of the added administrative burden argument and I think that may be one of the fears that Member States have about the Framework Decision, that this will add a big level of bureaucracy without necessary compensatory protection for individuals. All I can say is we are more than happy to look at those points, because we are concerned about that ourselves. Yes, there needs to be proper record-keeping but we have to draw the line. It is proportionality; the requirements have to be proportionate for what they are going to achieve.

Q179 ***Earl of Caithness:*** I would like to move you on to the ECHR and in particular Article 8(2) which requires that "the interference with the right to privacy be in accordance with the law". How can that be satisfied given the substantial differences between the Framework Decision and SIS II?
Mr Smith: I hope we covered that to some extent by the description of *lex specials* and *lex generalis*, and it is not one or the other. One sets the basic level, the Framework Decision, so that is what you get, what is in the Framework Decision, unless there is something better or more specific in the SIS decision. That packaged together should come up to the level specified in the ECHR and perhaps more specifically the Council of Europe Convention 108 on data protection. As I say, our concern is the way the Framework Decision appears to be going. That underlying level may be fairly low and then, if it is

low, there is a question as to whether or not it satisfies the requirements.

Q180 ***Earl of Caithness:*** That was going to be my follow-up question. Would you like to see the Framework Decision level increased?
Mr Smith: We do not know what is there at the moment. The only official text that we have ever had is the draft Framework Decision which was issued in June last year, which I think we were reasonably happy with. There is no doubt that it took account of the opinion of the European data protection authorities which they developed at the Krakow conference. It was a well-thought through measure. Our fear is that it has been picked to pieces and bits have been discarded. We do not know what has been discarded or what is left so we cannot comment on how satisfactory it is, but we are worried.

Q181 ***Earl of Listowel:*** In our earlier evidence this morning from the DCA we were hearing that the national authorities would be expected to be the enforcers and the European Data Protection Supervisor will have less stringent powers than the national authorities. In that context, will the national data protection authorities, particularly in the UK, have sufficient resources to carry out these supervisory responsibilities, particularly in the light of the lack of resources mentioned by the Commission in its report on the application of the Data Protection Directive? Can we really be confident that the new accession countries' national data supervisors will be sufficiently resourced to deal with these matters?
Mr Smith: I think some of the Member States do have real difficulties. We have an advantage in the UK that we have recently moved from the data protection functions of our office being funded through grant in aid. We are funded through the notification fee income that we receive and at the moment we are managing to increase that year-on-year, so it would be entirely wrong of me to complain about lack of resources for our data protection work. Like all things, there is an element of uncertainty because we are vulnerable if the fee income does fall off and it gets eaten away by inflation over the years because it is a set fee of £35. Also there could be more exemptions introduced through legislation which would cut the income, and I think this Schengen area is quite resource-intensive. The proposal is to meet twice a year. They are meetings in Brussels—that takes time and expense—there is the audit work to be undertaken, it talks about an information campaign, quite rightly, but that has to be funded, and an information campaign leads to more queries from individuals that have to be answered, so there is work there. I wonder if I might, my Lord Chairman, take the opportunity to comment on Schengen evaluations which you touched on?

Q182 ***Chairman:*** Yes, do, please.
Mr Smith: This has always been something of a mystery area. It is a mystery area to us where the legal basis for the Schengen evaluation comes from, but we have been involved in some Schengen evaluation activities because they evaluate a range of aspects: sea border controls, land border controls and data protection arrangements in Member States which are joining the Schengen System. There is a regular review of those which are already members, and we have taken part in some of the data protection ones. We were asked to lead the evaluations when the UK had the Presidency of the EU, and we did that to the Nordic countries, but we had to fund all of that from our own office funds whereas it was not bringing any real benefit at all to our office other than, you might say, it improved my personal experience and I found it extremely interesting. It was quite an expensive exercise, but if it is part of a process should it not be funded centrally? There is an advantage in those data protection inspections having people from data protection supervisory authorities with the expertise on them. There is also a question about how that evaluation process feeds into data protection supervision. It does not do so at the moment, but when we were looking at the Nordic countries we came across some general issues which could usefully have been fed back into the data protection supervision, some lessons that could have been learnt for all data protection authorities. There is no ready mechanism to feed that back, so if Schengen evaluation is to continue, there should be some link created between the process of Schengen evaluation as far as data protection is concerned, and the joint supervisory arrangements and regular meetings with the EDPS and so on. We think this would be extremely valuable.

Q183 ***Viscount Ullswater:*** I am sure the Information Commissioner's Office is directed to the protection of the individual and the individual's rights. Are you satisfied with the adequacy of the access rights for data subjects for the data held on them and whether some data perhaps is withheld on national security reasons?
Mr Smith: It is something we will look at and may come back to you on. We have not looked specifically at the access provisions in preparation for today but I have no reason to suppose that the access provisions, as they would apply in the UK, would be a problem. Individuals in the UK would make their application to SOCA. There is an ability to withhold information but only where providing it would be likely to prejudice the prevention or detection of crime, which is a test which is regularly applied, and

it is hard to see that with some of the articles like missing persons, how telling people that would cause prejudice. The danger is with the covert surveillance area which may well cause prejudice. We do not see, if you like, an obvious problem, it would be treated much like any police data would be treated in the UK at the moment.

Q184 ***Chairman:*** Mr Bamford, do you want to add to that?
Mr Bamford: No. I agree with my colleague there. I think at the moment the provisions of Article 50 are very much that the national law would apply in terms of the access rights so when we are going down these tiers of legislation yet again, we would be down at the UK Data Protection Act end of things, so the exceptions which are relevant there, potentially to the prevention and protection of crime, would kick in at that point. There is a relevant one to do with national security in particular instances, but it would be a situation which would be on all fours with general police information in the UK which we have managed with for many years.

Q185 ***Chairman:*** Can I thank you both very much indeed for coming to give evidence to us, you have been extremely helpful and given us very clear answers to our questions. If there is anything you want to follow up, please do feel free to do so. Can I ask you to pass on my thanks and regards to Richard Thomas for his written evidence which was extremely helpful. He has had a long and, from our point of view, extremely helpful correspondence with this Committee on previous inquiries as well, so please send him our regards.
Mr Smith: We will certainly do that. Thank you very much.
Chairman: Thank you kindly.

WEDNESDAY 1 NOVEMBER 2006

Present	Avebury, L	Henig, B
	Caithness, E	Marlesford, L
	Corbett of Castle Vale, L	Wright of Richmond, L (Chairman)
	Dubs, L	

Examination of Witnesses

Witnesses: MR PHILIP GEERING, Director of Policy, MS CARMEN DOWD, Head of Special Crime Division, Crown Prosecution Service, SUPERINTENDENT MIKE FLYNN, Director, Joint Operational Authority, SIRENE UK and MR ROB WAINWRIGHT, Head of International Department, the Serious Organised Crime Agency, examined.

Q186 ***Chairman:*** Good morning and welcome. Thank you very much for coming to give evidence to us. I want to explain at the start that this is on the record and being broadcast, and this inquiry is looking into the Second Schengen Information System. Perhaps I could ask you—and I do not mind in which order, but perhaps it would be polite to start with the lady—to introduce yourselves and tell us something briefly about what you do, what your organisation does and, as it were, where you come from?

Ms Dowd: I will ask Philip Geering to open on behalf of the CPS, if I may, and then if I may go on to explain my particular role within the CPS, if that is helpful? I think that would be more helpful to the Committee.

Q187 ***Chairman:*** Of course.

Mr Geering: My Lord Chairman, I am Philip Geering; I am Director of Policy for the Crown Prosecution Service Headquarters and I report directly to the DPP. Thank you for this invitation to us to give evidence; we welcome the opportunity on behalf of the Crown Prosecution Service to give evidence, as this is an important matter. We are particularly pleased to be appearing alongside our police colleagues, as this is a significant development for the CPS. I think the first point to make is that the Crown Prosecution Service, as the principal prosecuting authority within England and Wales, is not responsible for the setting-up and running of the SIS II system. However, we are significant beneficiaries of it and we work closely with our police and investigative colleagues to make it as effective as possible. In addition, the CPS will be providing some of the safeguards that will ensure the SIS system is used proportionately and appropriately. For example, some of the alerts will not be going on the system unless a Crown prosecutor has assessed the merits of that alert and approved the putting on of that alert. So this is a significant illustration of police and prosecutors working closely together to make for a more efficient and effective service to the public, and to victims and witnesses in particular, and at the end of the day enabling us to be more effective in bringing offenders to justice.

Q188 ***Lord Marlesford:*** Are you both barristers or solicitors?

Mr Geering: I am a barrister.

Ms Dowd: I am a barrister. I am sorry to interrupt, but if I may briefly explain that I am Head of the Special Crime Division and I have the operational responsibility for all matters pertaining to extradition cases, so when applications are made by foreign Member States for the return of fugitives to their State my team will deal with those applications.

Mr Wainwright: Good morning, my name is Rob Wainwright and I represent the Serious Organised Crime Agency, which you may know is a new agency established this year to fight serious and organised crime in this country. It opened its operations on 1 April this year following the passing of legislation through Parliament last year. My role in the organisation is to run the international affairs of the organisation, an international department that manages a significant set of international police cooperation measures on behalf of our own agency but also on behalf of all other UK law enforcements agencies. So we facilitate requests and assistance for international police cooperation on behalf of our partner agencies, and included in that framework, of course, are our plans for the Schengen Information System, and in particular the responsibility that we will inherit to manage the SIRENE Bureau of the Schengen Information System. So we are busy planning to build that bureau right now as an integrated part of our international work. We are, therefore, very keen advocates of the Schengen Information System; it will add important new capabilities to those that we already have and already offer to our partner agencies in the United Kingdom. Of course, some of the Schengen police cooperation measures that we have already adopted, such as the European Arrest Warrant and the cross-border surveillance measures under Schengen, are already with us now and are already playing an important role in our work. Of course, the establishment of the

Schengen Information System will increase that capability yet further.

Q189 ***Lord Marlesford:*** What is your background professionally?
Mr Wainwright: My background is as a civil servant; I have worked in a number of different departments in government.

Q190 ***Lord Marlesford:*** With the Home Office?
Mr Wainwright: With the Home Office and with the Ministry of Defence as well.

Q191 ***Lord Marlesford:*** Immediately before SOCA was set up?
Mr Wainwright: I was a member of one of the four precursor agencies of SOCA, in this case the National Criminal Intelligence Service.
Superintendent Flynn: My Lord Chairman, I am Superintendent Mike Flynn; I am from the Sussex Police. I run, on behalf of the end users of the Schengen Information System, the Joint Operational Authority, and that is the co-ordinating body with the Home Office programme for the end users across the UK law enforcement groups. My role encompasses everything from what it will look like on a police national computer screen, through to the operational guidance, the training and the rollout and co-ordination of the rollout for all the agencies in the UK.

Q192 ***Chairman:*** Can I ask for Lord Marlesford, what is your background?
Superintendent Flynn: My background is entirely in operational policing.

Q193 ***Chairman:*** Thank you all. You have had notice of some questions that we want to ask you, one of which you have already answered very helpfully, and I will leave it to you to decide which of you would like to answer the question, but it is open to any of you to come in after the first person has supplied an answer. Can you tell me, how much access will the Crown Prosecution Service or SOCA or other UK agencies or bodies have to SIS data? By SIS data I mean not only existing SIS data but also likely future SIS II data. Which bodies will have the capability or the responsibility of issuing different forms of alert and which bodies, or which of you, will have the responsibility to take action based on an alert? Who would like to have a shot at that first?
Superintendent Flynn: My Lord Chairman, access to the Schengen Information System is anticipated to be via the existing Police National Computer, and the access can be limited at organisational level. That is not all functionality of the PNC nor of the SIS will be available to every end user, and it can also be limited at individual user level within an organisation. Clearly not all PNC using agencies will be permitted to have access to the Schengen Information System, and access is very much limited by the Schengen Acquis Article 101. So it is very much to do with the function of the force or agency, and also the law enforcement business described therein; so it is about police checks, Customs' checks and border checks.

Q194 ***Chairman:*** When you say it will be limited, more limited for us than for Schengen members?
Superintendent Flynn: No, we take the same interpretation, except of course for Article 96 data, to which we do not have access. So the access depends very much on the force or agency and their access to the system. For example, some agencies do not have access to the vehicle database of the Police National Computer. There are three main areas to the Police National Computer: names, vehicles and property; and what happens, depending on the function of each agency, they have access to various areas of information. Also some agencies are able to update the system, for example police forces can do that, where they can update records on the system. Other agencies are entitled to search for data and act upon what they find but are not entitled to update the information. Essentially, if we did have an agency that wished to launch an alert on the SIS and they did not have an update facility then they would have to do it through partnership with SOCA and of course that would mean there would be an extra level of scrutiny regarding the importance and the relevance of the alert that they wished to raise. When it comes to responding to hits then any agency that actually gets a hit on an alert is expected to take the action requested. In those cases where the alert is not a prime function of the agency that gets the hit, for example if we were looking at missing persons and a Customs Officer, a Customs Officer's powers in relation to a missing person are actually quite limited. So what we have put in place are arrangements between ACPO and ACPO (Scotland) and the other agencies to ensure that prompt action is taken in those cases. There is also a question regarding the CPS; the CPS, as a primary prosecuting agency, would be entitled to have access to the data but at present they are not a PNC user, except for, I believe, one pilot that you are thinking of putting in place for CPS London, and that is to do with previous convictions information from the PNC and not from the SIS itself.

Q195 ***Chairman:*** Thank you very much. Would any of you like to add anything?

Mr Wainwright: Simply to add that SOCA as a national law enforcement agency will have full access in the same way as any other police forces in Europe, but will operate that access directly of course.
Mr Geering: I think only to add that we are entitled to have access but we do not really regard it as an operational necessity or appropriate. As far as we will benefit from the system we will be able to work through the investigators and they are best placed to operate the system. We do, as I have indicated, anticipate having an authorisation level to enable alerts to be placed, and that will reflect police prosecutors working closely together. So, for example, if an extradition alert is to be placed on the system ordinarily a prosecutor will have to approve that alert before it is placed, and in approving it the prosecutor will need to ensure that it is an extradition offence, that the code for Crown prosecutor tests are met—that is to say there is sufficient evidence and it is in the public interest to prosecute—and we will have to exercise some proportionality to make sure that it is an appropriate case to go on a European-wide network. So we will be providing that kind of safeguard. It applies in similar ways in relation to lost or stolen property, where the police might be seeking to put on an alert which will trigger a forensic examination of the property if it is recovered. That plainly has potential resource implications for other jurisdictions; this jurisdiction would not want to overload either the system or other countries with an inappropriate request and the prosecutors will be able to sign off saying, "Yes, that is an appropriate alert to place; we need the forensics on that property", or not, and the alert will follow, or not, as appropriate.
Chairman: Thank you very much. Lord Corbett first and then Lord Avebury.

Q196 ***Lord Corbett of Castle Vale:*** Superintendent Flynn, you reminded us that we do not have access to the Article 96 information on SIS, that is aliens who are refused entry. We have some figures here, 751,954 names on that. If we make a bilateral approach to the National Police Authority is it possible to get the information by that route on that basis?
Superintendent Flynn: I think if we were looking at a specific case we would work in partnership with the Serious Organised Crime Agency to make that request of another country, in a specific case; I do not think at this time we would expect them to send their entire updated list.

Q197 ***Lord Corbett of Castle Vale:*** This would be done presumably through Europol, possibly?
Mr Wainwright: That is certainly one significant mechanism that we operate. I said earlier that we have a range of instruments available, Interpol also; there is also a network of bilateral liaison officers that my agency has around the world. Of course every day we are cooperating with our partner agencies in Europe and beyond on the most significant operational cases, and some of that cooperation will involve access to the same information that, coincidentally, is also held on Article 96. So by our not having access to Article 96 by no means closes down all our avenues of possible cooperation in this area.
Chairman: Lord Avebury and then Lord Marlesford.

Q198 ***Lord Avebury:*** Mr Geering said that the CPS will ensure that alerts are only placed on the system when they satisfy the normal tests that a prosecution is viable. How do we know when you receive an alert that an equivalent test has been applied by another State?
Mr Wainwright: That is a key function of the SIRENE bureau, which we are developing in our agency. As I said, it is a very, very important function that we validate all incoming alerts from all other Member States against a standard set of criteria and common standards that apply right across Member States. It is a key function of our bureau to validate those in that way, as indeed it is for any outward alerts that the UK would be placing on the system.

Q199 ***Lord Marlesford:*** Can I just be clear in my own mind about the actually linkage, as it were, between the Police National Computer and the Schengen Information System. When you say that your agencies get their Schengen information through the Police National Computer, does that mean that there is a lot of SIS information on the Police National Computer, or is it that the Police National Computer has a facility for interrogating the Schengen computers?
Superintendent Flynn: Very much the latter. Essentially, although we have not decided the architecture of the UK's SIS II solution, it is most likely to be a national copy of the data that is held on the central European system, and that in the future, instead of a domestic inquiry from a police officer only interrogating one set of data, it will actually look in both databases for the information and will bring it back consolidated. You cannot take the European data and embed it into your national system—you are simply not allowed to.

Q200 ***Lord Marlesford:*** You say "will"—it is all "will"—so at the moment how do you get Schengen Information System under the present SIS?
Superintendent Flynn: We have no technical link to the current SIS.

Q201 ***Lord Marlesford:*** At all?
Superintendent Flynn: At all, and therefore a UK law enforcement officer cannot carry out an SIS check at this time.

Q202 ***Lord Marlesford:*** What is the date when you are going to be able to?
Superintendent Flynn: First of all, we have to have a central system in place and the latest guidance on that is that the central system is expected to be in place in 2008 and then the existing 15 Member States will have to migrate from SIS I to SIS II and then after that new Member States, of which the United Kingdom will be one, will have a staggered integration into the system, and we would reasonably expect this to be about 2010.
Chairman: Lord Dubs.

Q203 ***Lord Dubs:*** I wonder if I might go back to the Article 96 situation? You mentioned that you had other ways sometimes of accessing information, but in operational terms how much of a handicap is it not to have full access to Article 96 information?
Mr Wainwright: I think potentially it is a handicap, quite a significant one, and the government has always made a case to the Commission and other Member States that the United Kingdom, notwithstanding the fact that we are retaining our border controls, of course, should have access to the relevant part of the Article 96 database that concerns the movement of suspects of interest to us in terms of organised crime or counter-terrorism. So if it were possible, technically and administratively, to delineate with that database the difference between that information that is on there purely for immigration control purposes and also that on there for the control of suspects entering the EU, then we certainly would want access to the latter, and we have been arguing the case for a technical solution to be brought to bear as part of SIS II that can allow us to participate in that way. It is very much in our interests but other Member States agree that it is in their interests as well because the UK is a very significant part of the European Union's response, of course, to fighting terrorism.

Q204 ***Lord Dubs:*** May I ask you this, what preparations have you made—that is the CPS, SOCA and the SIRENE office—to date for the application of SIS and SIS II and what further preparations do you still need to make? I know you have referred to this partly.
Mr Wainwright: Maybe I can expand my earlier answer, thank you. The precursor agency of SOCA responsible for this work was the National Criminal Intelligence Service, of which I was a member, as I said earlier, so I have had personal experience of being involved in this work now for a number of years. NCIS, that agency, participated with the Home Office in particular and other agencies in the development of our SIS I preparations, and we expected SIS I to go live in this country probably by 2005 at the latest. As you know, for other reasons, technical and otherwise, that was not possible in the end, but at the time we had prepared quite strongly and in detailed form in NCIS for our SIRENE bureau functions. So that involved technical preparation, working with Home Office colleagues, working with the technical integration with the Police National Computer, but also recruiting a body of staff to staff the new SIRENE bureau. So we recruited the staff and we trained them. As it happens, we do not have SIS I application but we still have the staff and that is good for us because we still have now the other police cooperation measures of the Schengen Agreement that we are operating, such as the European Arrest Warrant. So we can use that staff and the body of expertise and experience that we have had now of course to good effect as we prepare for SIS II and the SIRENE bureau under SIS II, which will be different in some ways but in many ways we are dealing with the same issues. So building on that body of experience, using the staff, the training path that we already have, we are preparing for our signing up to SIS II and I have every reason to believe that we will have a fully functioning highly capable SIRENE bureau as part of that.

Q205 ***Chairman:*** This Committee has heard a lot of evidence about the delays in implementing SIS II. Have you, from your point of view, been very conscious of these delays and are they causing you problems?
Mr Wainwright: Only in the sense that the longer we take as a country to sign up to SIS II the longer we have to wait to add a powerful new capability to our law enforcement powers in this country, of course. So to that end, to the extent to which I represent the wider interests of UK law enforcement, then, of course, it gives me cause for concern, as it does in other parts of government.

Q206 ***Lord Dubs:*** You have partly dealt with my next question, but in case there is anything you want to add. What will be the effect of SIS II on the operational efficiency of UK law enforcement agencies and criminal justice bodies? And from an operational perspective, what added value will SIS II offer compared to the current SIS I?
Mr Wainwright: Whilst Mike is finding his note perhaps I can summarise it from our perspective? The use of biometric data in particular, which in many respects represents a very strong future capability in law enforcement, so SIS II is planning on the basis

that we can use biometric data. The technical capability for that is not yet ready but when it is then of course it gives us a powerful new tool against searching, against records. SIS II also brings the capability to add new alerts, not just those limited to people and a certain small number of objects as they are currently but also new objects such as boats and parts of boats and also parts of aircraft. Also, importantly, new analytical capabilities to link different alerts and to provide the operator, therefore, with pointers as to where the investigation should lead in terms of linking different persons and objects. Have I missed anything?
Superintendent Flynn: That is very comprehensive!
Mr Geering: If I may add from a prosecutor's perspective to this question, I would endorse what Mr Wainwright has said about this being a powerful new tool. It has considerable potential from the perspective of the prosecutor. As we reform the CPS from a reactive paper-based organisation into one that fully understands its public service role and its function in bringing offenders to justice, we turn our prosecutors into proactive operators. If I can illustrate that. At the moment, if a suspect goes missing then we file our papers and wait for them to turn up; if we believe that they may have gone to Europe, if we have intelligence understanding of that from the police, then we may prepare a European Arrest Warrant and that will be sent to the country where we think they are, and then we will hope that they are found and brought back. SIS II has the potential to turn that, an essentially reactive mode, into a proactive mode. If we have reason to believe that the person has gone to Europe or is within Europe and we want them found then we can, working with our police and investigative colleagues, get an alert on to the system. This is a much more proactive opportunity for us in bringing offenders to justice and it has great potential and is really quite exciting in terms of law enforcement. Reverting to the point about preparation, we have worked very closely with SIRENE and with ACPO to prepare. We prepared for SIS I, a Memoranda of Understanding was signed between the CPS and ACPO; draft operational guidance was prepared—and that of course was shelved when SIS I and was not pursued. We will pick that up, we are picking that up again with our colleagues and partners. We will refresh it—I do not anticipate any significant change—and particularly in relation to the operational guidance that indicates that prosecutors will be authorising certain alerts. So we will train and prepare our prosecutors so that we can deliver on the effectiveness of SIS II. Of course, that inevitably prompts a resources implication. We would anticipate an increase in caseload because of SIS II. We anticipate that first of all because we have seen an increase in caseload in relation to the European Arrest Warrant and that has been a positive step forward—and I will revert in a moment to my colleague, Ms Dowd, to perhaps develop on this—but also in looking at other jurisdictions where the SIS system has already been introduced. Clear evidence of escalating caseload, good in terms of public service and bringing offenders to justice, getting resolution for victims and enabling witnesses to give evidence as quickly as possible. But of course it carries the resource implication.

Q207 ***Chairman:*** Do you want to pick up that invitation?
Ms Dowd: My Lord Chairman, just to clarify that in assessing the resource implications in 2003 it was evident that on any estimation that the likely impact on caseload was that it would increase significantly. It has actually been borne out that the European Arrest Warrants have increased our workload across the board, save actually in relation to the import extraditions, i.e. where we are still in reactive mode in terms of knowing where people are and making applications.

Q208 ***Lord Corbett of Castle Vale:*** Do you know by how much? Is that an extra 10 per cent or 20 per cent?
Ms Dowd: The estimate for the end of 2006 is that we think our caseload would have doubled from 2005, and that is across the board in relation to all extraditions, not just European Arrest Warrants. So a lot of preparation needs to be made in relation to further resourcing issues once SIS II is implemented, and we have to take that forward with the Home Office and have some negotiations around that.

Q209 ***Chairman:*** How much is that increase in workload due to enlargement and the recent new Members of the European Community?
Ms Dowd: Certainly a significant number are due to that, but there are other issues at play in relation to the rest of the world, so I cannot say that it can be totally accounted for in relation to that.

Q210 ***Chairman:*** Do you have any perspective on how ready Bulgaria and Romania are, coming into the scheme? This is rather beyond your remit.
Mr Wainwright: In terms of the European Arrest Warrant I believe that actually they are quite ready and they may be ready as soon as 1 January when they accede; I think there is still some technical work to do, but I think they are quite ready. If I can add to the point that my colleague made? The use of the European Arrest Warrant certainly increased the workloads in my organisation and in others as well, but it really has delivered significant new benefits, I have to say. It is a hugely important new tool for police officers and the ability to track down very

quickly fugitives from justice and to return them to British jurisdiction much, much more quickly and in a much simpler way than ever before really does add a powerful new capability. I am aware of several high profile cases already where we have helped ourselves in Europe, where we have helped our European partners by apprehending important serious crime figures in the United Kingdom. This is a very good news story for policing; I have to say, notwithstanding the fact that it increases the burden of some of our work.
Chairman: Thank you. This Committee likes good stories!

Q211 ***Lord Marlesford:*** Just to follow that up, can you give us a feel for size as to how many European Arrest Warrants has the UK issued in whatever the most convenient last year period?
Mr Wainwright: I do not know, I am afraid, my Lord. My colleague might be able to help you.
Chairman: Incidentally, I should say that if, at any point, particularly when you receive the transcript of this meeting, if there are any points that you think it would be helpful for us to have supplemented in writing, please feel absolutely free to send us in additional evidence.
Lord Corbett of Castle Vale: Would it be unfair to ask you to add a note on information on how many requests for warrants from other European States you have responded to, because it is a two-way street?

Q212 ***Chairman:*** Can we put those questions on the record?
Ms Dowd: My Lord Chairman, can I briefly come back to your questions about Bulgaria and Romania? Our experience in the CPS is that the new EAW countries are generally well prepared and respond quickly to requests for further information, so our experience is a very positive one thus far.

Q213 ***Chairman:*** That is very interesting, thank you.
Mr Wainwright: I have some of the details now, thank you. Between January 2004 and August of this year, since the European Arrest Warrant has been functioning, we have issued a total of 307 European Arrest Warrants in the United Kingdom on behalf of our partners in the EU, which has led to the arrest of a total number of suspects of 172. So that gives you a feel for how much work we are doing, and there is a corresponding number that we are seeking cooperation for in other parts of Europe.

Q214 ***Lord Marlesford:*** Is that the one that Lord Corbett asked about, in other words requests made of us to arrest people?
Mr Wainwright: Yes.

Q215 ***Lord Marlesford:*** And you do not have, at the moment, the figures for the number of requests we have made into Europe for arrests?
Mr Wainwright: I am sorry, I think I misled you. I think that is the result, that is the number that we have sought assistance from our European colleagues.

Q216 ***Lord Marlesford:*** So the figures again were?
Superintendent Flynn: 307 warrants issued, which is outgoing requests, and 172 people arrested because of that.
Mr Wainwright: I should validate those figures and I can provide you with more accurate figures and indeed more up to date figures after the Committee.
Chairman: Thank you. Lord Avebury.

Q217 ***Lord Avebury:*** We have been concentrating on the increase in the workload arising from the European Arrest Warrant, but the real step increase will surely take place when SIRENE goes live and that will not be until 2010. Have you already had any discussions about budgetary implications and can you give us an idea of the order of magnitude of the resources that will be needed by SOCA and the CPS?
Mr Wainwright: We are still working on the volumetrics on that, as you can imagine, but based on the experience of our partners in the European Union we expect this to have a significant impact on our workload, maybe as much as twice or even three times as much in terms of the handling of the data that we currently manage through our cooperation channels. It will have a significant impact, absolutely. Our response to that, including in terms of providing increased budgetary provisions, is something that we are currently discussing with the Home Office, and of course something that I am discussing with my own Director General.

Q218 ***Chairman:*** Clearly what we are talking about is a formidable amount of IT communication. Have any of you had serious IT problems in terms of actually communicating all this information?
Superintendent Flynn: The existing system, SIS I, copes with the amount of traffic. The UK will provide a considerable amount of traffic when we go live but the estimate of the amount of information exchange brought by the ten new Member States to the EU is essentially about the equivalent of what Germany provides today. So on that it is anticipated that the updated network which is being put in place now should easily be able to cope with the exchange. It is dealing with the business at the end that is the big question. From our point of view, yes, we do anticipate that there will be more work for police officers on the street, but it is actually good news because this is getting hits on people, on stolen

property that hitherto we could not get. Without the Schengen Information System there is no joined-up way of receiving and managing the information and allowing police officers at street level to be able to check a German vehicle and find out if it was stolen, enter a premises, find a dozen passports and be able to do a check from the premises to see if these passports are stolen. So for us it is quite a revolution.

Q219 ***Lord Corbett of Castle Vale:*** Is it not the case that as bad as the absence of information, as bad is inaccurate information? This touches on resources. Are you satisfied that you are making progress and getting this understood in the Home Office? If a backlog builds up, like the Criminal Records Bureau, we are all in the soup.
Mr Wainwright: Absolutely, but in answer directly to your question I am satisfied that this point is well seized at the Home Office.

Q220 ***Lord Corbett of Castle Vale:*** Can you say whether there is any statistical data available on the use of SIS and SIRENE by other Member States? Is there any information available on the number of complaints made about inaccurate data and other exercise of data protection rights in other Member States? What is the experience so far on the ground?
Superintendent Flynn: First of all, regarding the use of the system I have brought along the statistics for the amount of alerts on the existing system as of midnight on 17 October. I can provide these to you because it covers all the alerts and all the Member States. I have also brought along the latest set of statistics regarding the number of hits as reported by the various SIRENE bureaux around Europe, and, again, that breaks it down by country, by year and by Article. So we can actually illustrate the amount of use and the amount of success that they get from the system.

Q221 ***Chairman:*** If you are prepared to leave that with us afterwards it would be very helpful; or send it to us.
Superintendent Flynn: I think I am entitled to, yes. Then regarding complaints, there is not any standard reporting of complaints regarding data protection inquiries because each Member State deals with them in their own way and it could well be that a complainant or an inquirer will get in touch with the data owner in the actual country, so they could be getting in touch either with a SIRENE bureau or they could be getting in touch with a police force or a Customs agency without any reference to their Information Commissioner, and so there is no central reporting. I got in touch with the member of the Council in Brussels who liaises with the Joint Supervisory Authority, which is the co-ordinated data protection mechanism. He said that there were no central statistics available, but anecdotally he said that the bulk of the small number of complaints that there are are really queries regarding Article 96, and this is where people have tried to get a visa to enter the Schengen area, have found that they are on the system and wish to query why they are on the system. So that is the extent of the reporting so far.

Q222 ***Lord Corbett of Castle Vale:*** In September the Commission adopted a new version of the SIRENE manual which governs the exchange of supplementary information between Member States. Do you know why this text has not been made public and are you aware of any significant changes having been made to the previous version? Do you anticipate whether further changes will have to be made in the light of SIS II?
Mr Wainwright: Yes, I think you are referring to the updated SIRENE manual for SIS I Plus, I think it is, which was adopted, as you say, earlier in the year. As we are not members of SIS currently of course we were not party to the drafting of that manual and did not receive an official copy, nor should we have, although we have now of course been given a copy, if you like, as an information addressee. I understand that it has not been made public because the Annex to the document is classified the equivalent of UK restricted, and that is because it has the contact details of SIRENE bureaux and their officers and that is classified in the way I have described. A draft of the SIS II manual is currently underway and is expected to be issued by January next year—so quite soon now—and is likely to be adopted in April or May of next year. We are involved in that drafting committee work and in fact we do anticipate in that case that that particular manual will be made publicly available.

Q223 ***Lord Corbett of Castle Vale:*** Are you aware of any changes between the two? Are there major changes or is it tidying up?
Mr Wainwright: I think it is mainly tidying up; there are no significant changes.
Chairman: Baroness Henig.
Baroness Henig: I think you have covered what I was going to ask in Mr Geering's opening statement. I do not know if you want more detail?
Chairman: No, thank you. Lord Avebury.

Q224 ***Lord Avebury:*** Could we turn to the question of biometric information and what is currently taken from persons in the UK for criminal justice and law enforcement purposes, and could you say what the process will be for transmitting this information to SIS II? Will the UK procedures for taking biometric

information be amended in the light of the planned application of SIS II?

Superintendent Flynn: My Lord Chairman, essentially fingerprints and photographs are taken either by consent during investigation or from suspects when they are detained at a police station in consequence of being arrested for a recordable offence or when another legal requirement exists for them to be provided. It is envisaged at this stage that biometric information—we talk about fingerprints in the first instance—would be posted centrally on to the SIS and linked to an alert, and really in this case we are largely looking at extradition alerts. We would do that from the National Automated Fingerprint Identification System that exists in the UK. It is possible that we could provide fingerprints for specific vulnerable missing person cases as well and possibly photographs. There is no intention of routinely circulating on the SIS any other biometric records; we have to keep a strict separation between the national system and the Schengen Information System. So ideally we would be looking at a situation in the first instance where somebody is arrested, they give their details to a police officer in whichever country they happen to be; there is then the opportunity of being able to download from a central system the link to fingerprints to confirm the identity. So that is how it is envisaged in the first instance. What they are then considering is whether we will be able to use them for identification purposes, which we consider to be particularly valuable because we know that criminals tend to lie about their identity and therefore it would be much more useful to be able to check their fingerprints. We do use the National Automated Fingerprint Identification System; the intention is that when either somebody is arrested or when there is an incoming European Arrest Warrant, there will be the opportunity to check whether we already know this person, whether we know them by that identity, and sometimes it might even be, where they are. For example, they could already be in custody and it would be useful to be able to flag that up. At this time, if you are talking about photographs, although there is a project underway, and that is the Facial Image National Database, that is only building the database at this time so we have no method at this time of linking that to the SIS. Prior to the identification side going live, that is where we have somebody in custody and we would look to identify them primarily from their fingerprints, there would be European Parliamentary scrutiny of this and the Commission will actually put forward a report regarding the availability of technology and the reliability of the technology to allow us to make that important step, and we do view that as a very important step. Regarding how it actually works, in the UK we use a technology called "Livescan", which in many ways looks like a sophisticated photocopier. It is much more reliable than the old ink fingerprints and essentially takes a scan of the fingerprints to a much higher quality than we were able to do before. That then gives you an initial feedback as to whether you have a match and a high, medium and low success rating. If the person protests that it is not them, even though we have a match on the system, there is a further stage where we actually go to a fingerprint expert and the fingerprint expert carries out a check on the prints as well. That is most important, to get the identity right, not to inconvenience people, and we can actually turn those around typically in about an hour and 20 minutes, which, again, is much faster than we were able to do with ink fingerprints. Is there anything else you would like to know about the system?

Q225 ***Lord Avebury:*** I would like to ask you in particular about the use of DNA profiles. We have the largest DNA database in the world, I understand. Is there any suggestion that that can be used in SIS II?

Superintendent Flynn: At this time it is not actually within the design; they are looking at fingerprints and photographs. Although I think looking to the future it would be extremely sensible to look at the availability of DNA profiling to be able to exchange between Member States, but initially we are looking at fingerprints and photographs.

Q226 ***Lord Avebury:*** Could you then say how the UK procedure for taking biometric information compares with the procedure in other Member States and whether there will be standard rules on the enrolment of biometric data, so as to make it comparable between Member States, and will that require any changes in UK practice?

Superintendent Flynn: On that one, the UK is actually something of a leader in biometric information, but there are discussions between the Member States regarding standards, and I know that my colleagues in SOCA work with Interpol on establishing standards for photographs, fingerprints, and, again, we will be looking at international standards on DNA. So on that one, there are working groups where we agree the standards. As far as we are concerned we are already well in advance of these and therefore we collaborate with our other Member States to ensure that we are working to the same standard, but they are usually the internationally agreed standards that we all work to.

Mr Wainwright: Although I have to say that practices are rather different so in some Member States biometric data is taken for administrative purposes to support a national ID card system, for example, whereas, as Superintendent Flynn has said already this morning, in the UK we only take it by judicial

authority. So there is an important difference. But the application of those standards in SIS will not require any changes to the UK system.

Q227 ***Lord Avebury:*** I am conscious of the fact that some of the questions we are asking you ought to be dealt with on the SIRENE website, which I had a look at, and there is a *Frequently Asked Questions* page there, but there are not any links from the *Frequently Asked Questions* page to the answers. Are you planning to expand the SIRENE website so that that will be remedied?
Superintendent Flynn: Thank you for that feedback; we will make sure that is changed! Yes, we will update it. We do not want to necessarily get expectations up as we are going through a relatively long project, but the communications and marketing strategy, at that time will be put in place to make sure that people are aware of this new initiative. Then when we do get questions coming into the website, if we get them often enough we can extend the *Frequently Asked Questions* page.

Q228 ***Chairman:*** Can I just go back to fingerprints for a moment? How often is there a false match in fingerprint identification? Give me a rough idea, both from our practice and, indeed, if you know it, from SIS's practice?
Superintendent Flynn: Thank you, my Lord Chairman. On that one I discussed this issue with the director in the police IT organisation, and what you can do on a fingerprint system is you can change the algorithms regarding the sensitivity, so that in fact you would get no false hits but actually you would miss something where the computer was 99.9 per cent certain that it was that person. So there was a balance to be struck; that is why you get the high, medium, low response, and if there is any further doubt you go to the verified ID stage, where you go to a fingerprint expert. So to actually talk about percentages can be quite difficult and misleading because you can actually vary the accuracy of the sensors.

Q229 ***Lord Marlesford:*** Following up on that, if I may, for example when one comes into the US now one has one's fingerprints taken immediately. They presumably have those on some sort of database.
Mr Wainwright: Yes.

Q230 ***Lord Marlesford:*** Is that database available to SIS or to us?
Mr Wainwright: It is not available to SIS because of course the United States is outside the European Union, but it is available to UK law enforcement through other cooperation channels that my organisation operate.

Q231 ***Chairman:*** Can we turn to flagging alerts, and you may have to explain to me what I mean! In what circumstances will the UK authorities be flagging alerts so as to prevent action taking place on the basis of the alerts? How does this compare with the practice of our fellow Member States and will their practices be likely to change with the application of SIS II, in particular in those Member States where the European Arrest Warrant is currently inapplicable. Do you understand that question and can you give me an answer to it?
Superintendent Flynn: We will try! First of all, I will deal with flags. On the system there are flags which are essentially markers for each Member State and when an alert arrives in that Member State and they validate it, it might be that for certain reasons they cannot action that alert. They would then get in touch with the UK SIRENE bureau or whichever SIRENE bureau had launched the alert and ask for their flag to be set against it, and it just means that they will not be seeking to take the action that we have requested.
Mr Wainwright: Indeed, most grounds for flagging in the system to date have been around what is Article 95 alerts, which have since of course been replaced by the European Arrest Warrants, so most of the flags we used in the past around extradition requests, the European Arrest Warrant provisions now supersede that and so the grounds for the majority in the past have now been taken away. It is still possible, of course, to flag in other areas, particularly around missing persons and also the Article that deals with the need for discreet checks, for example, discreet surveillance of a subject, so it is still possible to do that, but the amount of flagging that is now done in the system is considerably lower.

Q232 ***Chairman:*** Can you give me an example of flagging? Would it be your concern that action might in fact ruin a surveillance operation?
Mr Wainwright: Quite, that is a very good example and there might be others that Mike can provide.
Superintendent Flynn: A lot of this is still under discussion for SIS II as they decide whether there will be automatic changes of action requested or flags put on the system, but, say, for example, we launched an alert for a vulnerable missing person, they were found in another Member State and within their national law they had to make an assessment as to whether this person was suffering from a psychiatric condition that rendered them vulnerable. Their specialists disagree with our view, therefore they cannot, under their national law, do what we ask; they would then get in touch with us because they would not want the person to walk out, be stopped by the next police officer and the same action commenced again. So they would ask that a flag be set on that so that they

did not do it. Similarly, there are some countries where, if you ask for a specific check as opposed to a discreet check, they would say that actually under their law they are not empowered to do that and therefore they would automatically want to turn all the requests for specific checks into discreet checks.

Q233 ***Baroness Henig:*** I think I understand, so the flag is issued when the UK issues an alert, and then it is flagged if the other country cannot take action. But is that time-limited? Maybe they could take action next year, or how long does the flag stay on? Is that it, is that forever?
Superintendent Flynn: If they cannot take the action or, for example, we had sent an extradition request and it was missing a key piece of detail, they might ask for that piece of detail but in the interim they would flag the alert pending us sending the information through, so that they could then ask for their flag to be removed.

Q234 ***Baroness Henig:*** So there are different categories of flags?
Superintendent Flynn: Again, much of this is under discussion as to how it will work in SIS II and whether we will have flags or automatic changes.

Q235 ***Lord Corbett of Castle Vale:*** You want to talk to the Royal Navy!
Superintendent Flynn: But on this one the general theme is that if temporarily or permanently they cannot do something that we ask there is some way of marking the record so that law enforcement officers do not take the action that we have requested.
Baroness Henig: I am thinking that it might be useful to differentiate between the temporary and the "that is it" one.

Q236 ***Earl of Caithness:*** I want to ask about the working operation for the law enforcement officer? At the moment there is a difference between the wording in the framework directive and in SIS II about information that is taken for national use and information that is spread between Member States. How is the law enforcement officer actually going to operate this in practice when he is taking data on a national basis under one criteria, only to find that in due course that information is then sent abroad to the SIS II system and is hawked around the other Member States?
Superintendent Flynn: Are we talking about the creation of an alert, or the response to an alert?

Q237 ***Earl of Caithness:*** Tell me the answer to both of those.
Superintendent Flynn: What we have done essentially between ACPO and ACPO(S), SOCA and the Crown Prosecution Service, we have worked out end-to-end business processes and rules regarding the creation of alerts. Some alerts we would describe as optional: that is, not every wanted person on the Police National Computer goes to the Schengen Information System; it is only those where we have been through the business rules and we have agreed that there will be an European Arrest Warrant, there is CPS approval, there is SIRENE bureau validation and off it goes. So from that it is a strict business process. There are others, such as stolen motor vehicles, where any reported stolen motor vehicle in the UK that is placed on the Police National Computer will go to the Schengen Information System because we could not put in place any justifiable business rules saying that we will only put valuable cars on the system, because we found from talking to our partners in the other Member States that quite often it will be low value cars that were stolen and were exported *en masse* perhaps across Europe towards the Balkans where there was a ready market for them. So in these areas, where we simply could not justify it to ourselves or the public, putting some kind of barring, what we are saying is that every stolen motor vehicle, firearm, trailer that meets the rules that goes on to the Police National Computer will automatically go to the SIS, and if it is found it will be automatically cancelled. Again, we have put in some very strict weeding rules to ensure that we do not leave data lying around.

Q238 ***Earl of Caithness:*** Does this pose any operational difficulties for the policemen?
Superintendent Flynn: No, because national law applies. In this one national law applies and if they come across, for example, a stolen German motor vehicle then essentially the system will give them some information, tell them what to do and tell them where to get some more information and that is via the SIRENE bureau. And then as soon as you are into the international liaison and cooperation we rely on the work of the SIRENE bureau to ensure that the officer operates within national law and that any international liaison goes to the SIRENE bureau.
Mr Wainwright: If I may add, I think this is about levels of confidence that police officers have between themselves, not just within the UK but around the European Union, of course, and I think, depending on the sensitivity of the case, one would expect a British police officer to have every confidence in their European colleague in terms of handling his or her case, and indeed we would expect significant benefits to be derived from that, and most police officers would want to know, of course, if a German or a Spanish colleague has stopped a stolen vehicle as part

of his or her case. Where the case becomes more sensitive then there are other channels for our cooperating with our European colleagues, particularly with Europol, for example, where we can exercise much more control over the extent to which information is shared with colleagues. But we do work on the fundamental principle that there is a level of confidence naturally within the European Union, within which we can each benefit of course.
Superintendent Flynn: One of the huge advantages we have is the decision made within SOCA to ensure that from the law enforcement point of view we have a one-stop shop, and that is, if there is an angle that requires Interpol or Europol or the use of the Schengen Information System, you are actually dealing with the same place all the time and the staff within the SIRENE bureau are actually able to work out which route this inquiry should take. And within the business rules—say, for example, on a sensitive issue, we are asking for a discreet check to be made on a serious criminal—then in-house we ensure that all those alerts will go through a force intelligence bureau where the sensitivity can be gauged before we go forward and liaise with the SIRENE bureau.

Q239 ***Lord Dubs:*** It is not a question of which you have had notice, so bear with me. As a Committee, we looked some time ago in a previous study at Europol and Interpol. Is it clear what the links are between SIS and Europol and are there any difficulties as regards a possible overlap with Interpol?
Mr Wainwright: With Europol, we do support the position which most Member States favour, that Europol should have access to the SIS II database—that is not yet the case—exactly for the reason that you alluded to, which is so that we can manage the potential for any cross-overs of information between cases that Europol are working on and those SIS II have. In the majority of cases, however, the two are dealing with a different level of sensitivity, a different type of casework. Europol is much less about volume casework, of the type SIS is, and much more about quality casework around serious crime, including counter-terrorist cases. Interpol however does deal more in volume casework so there is a potential for there being a duplication there. Of course, Interpol operates worldwide and SIS is just a European capability. The management of the data between Interpol and SIS is a bit more complex because of the particular framework within which SIS is managed, which is distinctly European Union; whereas Interpol of course operate on an entirely different basis. There are however parts to the Interpol programme—for example, on DNA that you mentioned earlier and on stolen passports—that do have a natural connection with SIS II and, in that case, I think it has to be worked on a national level rather than through the central European framework of SIS II.

Q240 ***Lord Marlesford:*** The decision on SIS II will allow the processing of data, other than for the purposes of acting on alerts, in exceptional circumstances. What use do UK authorities intend to make of this?
Superintendent Flynn: At the moment it is difficult to envisage the use of the SIS in this way without looking at a particular set of circumstances on which to answer the question. Because SIS is very much a hit/no hit system where we are looking for specific individuals and we have a match or we do not have a match, there is very limited descriptive detail held in a Schengen alert. It does not lend itself very readily to investigative purposes. The reason for that is that the system is, we describe it as, table driven. Because in the UK we want it to appear in English on our screens and in Finland in Finnish, it is based on code tables, so you get a specific value and that value is translated into whichever is the language of the host nation. That limits the amount of detail you have in the system. I will try to think of an example. Say, for example, we had a terrorist outrage and we had a description of a potential suspect. The first thing we would do is look for somebody with those features within the police national computer, but if we were looking at a case like that we would immediately go to our colleagues in SOCA and ask for bilateral communication with the other Member States because we would be much more likely to get a match from them searching within their national systems than any opportunity to go trawling in the SIS, because the SIS is not at all sophisticated in that respect. The procedures are already in place. If we asked France and Germany if they would search their national systems for somebody of a certain description, we would go through SOCA to achieve this and the exchanges of information are already in place. Another example might be we would be looking for a silver Mercedes. We have half the index number. Nationally, we could search against the UK databases to see if we could find a silver Mercedes with a number like that. It would not be a reliable thing to do to search the SIS for that because the SIS only has stolen motor vehicles in there and not a complete vehicle database. Again, we would go to SOCA and establish bilateral communication to see if we could get other Member States to deal with that. Regarding incoming requests, these would be requests probably coming in through SOCA where SOCA would then contact the owners of the information. That could be one of the constabularies or one of the agencies. Again, in individual circumstances, if we were assisting another country with an investigation and they had set out the

circumstances, the rules are already in place for the authorisations and exchanges of information. Again, we would use SOCA as our gateway. The issue for us here is that SIS is a compensatory measure for the removal of frontier controls and therefore it is very much a border focused, one-to-one match, hit/no hit system as opposed to a huge database that you would want to go trawling in for investigative purposes. It may be in future that we could agree with other Member States that there would be purposes we could use it for. The discreet check and specific check alerts, for example, clearly do have an investigative angle because you are looking to use those to trace the movements of people, linked vehicles and in the future linked containers, aircraft and vessels. There obviously is a move towards investigative in that area but I think there are much more reliable databases and partnerships already in place to allow us to do that.

Q241 ***Lord Marlesford:*** To recap, we should always be thinking of SIS as a system of data for border control in one form or another and other investigations, be they criminal or terrorist or missing persons, are primarily done through other agencies, particularly SOCA?
Superintendent Flynn: Yes, for border controls but I think very much for police and Customs checks carried out on your territory, because it gives you the opportunity to check if something is lost or stolen, if somebody is wanted or missing. Those are the types of purposes. It finds people and property that are of interest now. It does not have any history to it. If you want to go further on an investigation, then it is more reliable to establish a bilateral relationship via SOCA to do that. SIS tells you about people and property that are of interest to Member States now.

Q242 ***Lord Marlesford:*** Going back to the American system of fingerprints at borders, in theory a UK law enforcement agency could ask the Americans, if they had a fingerprint of a particular person and they wanted to know whether it had arrived in the United States, "Can you check whether this person has recorded fingerprints on entry within this particular period?"
Mr Wainwright: Yes, we certainly could and we do.

Q243 ***Lord Marlesford:*** Do any other countries take fingerprints at the borders of the EU? Do any EU countries take fingerprints when you arrive?
Mr Wainwright: I am not aware of any but I may be mistaken.

Q244 ***Lord Marlesford:*** When they now swipe passports in most European countries, is that swipe recorded? It is after all essentially a Schengen information factor. Is that swipe recorded and therefore available? In other words, if you wanted to know if I had gone to Portugal, would you be able to say to the Portuguese, "Has Marlesford's passport been swiped?"?
Superintendent Flynn: I think that might be an example of where you are looking at a specific person or a specific case and you would then go and ask for the permission of that country: "Do you have this information and within your legislation how would you release it to us?" It would be very much on a specific inquiry that you would be looking to get that rather than, "Please trawl your databases and tell us anything you find." On that, one would be pursuing an investigation and because of that it is very much not a general trawl of the system. We are asking somebody, "Do you have this information and are you entitled to release it to us?"

Q245 ***Chairman:*** What if the SIS data becomes interoperable with other databases like Eurodac, for instance? Does this have implications for us?
Mr Wainwright: It does. I can only think of positive ones in terms of increasing yet further the field of view effectively and cross-matching.

Q246 ***Earl of Caithness:*** Given what you have said about the increase of benefit that SIS II will bring to you, what operational procedures are being instituted within the UK as well as other Member States, to your knowledge, to stop fishing expeditions and to concentrate on going for alerts and hits? With a bigger and better system, is there not a temptation to go on fishing expeditions?
Mr Wainwright: I think there is that danger. You are absolutely right. Again, you are relying on the integrity of police officers in the Union. It is compensated by the fact however that a substantial part of the information relating to a particular case—certainly any sensitive information relating to that—is not stored at the front end. It is not available to the operator. It is stored as part of the SIRENE Bureau and the access and the backup that the SIRENE Bureau has. That gives us a measure of control over the most sensitive parts of the information.

Q247 ***Chairman:*** Can I now ask a question of the Crown Prosecution Service? You said that SIS II was likely to be very important for you but I think we have the impression from the answers to our questions that in fact bilateral activity is probably at the moment more important to us than SIS links. Would you like to comment on that or indeed would you like to add anything else, because I think the bulk of the answers have tended to come from that side of the table and I am not sure that we have given you sufficient opportunity to express your views.

Mr Geering: We anticipated that balance because the responsibility for setting up and running SIS and the links with other foreign jurisdictions is very much with the police and SOCA. We anticipated taking a lesser role, so no offence taken. Before SIS is up and running, the bilateral arrangements that we have within Europe are essential to plug the gap. The point is that SIS would provide a blanket, central European opportunity to put out an alert. At the moment we can only target the country where we think the suspect might be and not cover Europe in a blanket fashion; whereas SIS will provide that blanket coverage. If we were wrong and they had not gone to France but in fact had gone to Germany, we would still pick them up. That is pretty exciting in terms of prosecutors being able to take cases to court. We spend all this time conducting investigations, preparing a prosecution, lining up the witnesses. We are all ready to go to court and have a trial to bring some justice, a guilty or not guilty verdict, and the one person who really matters who preferably needs to be there—I suppose who has the least interest in being there—chooses to abscond. We cannot allow the system to be held up in that way. People do abscond and at the moment we rely on these bilateral arrangements to attempt to identify them, trace them and bring them back. SIS will give us a more proactive opportunity for tracing these people, having them located and brought back. In a way, that will be achieved more often and faster than current capabilities. That is really important. The sooner cases are brought to court the better, the better for victims to see some resolution of the matter, the better for witnesses whose memories will be fading and the better for the public to have confidence that the system is actually doing the job. That is very much what we want. That has been very much at the core of the reform of the CPS in the past couple of years under this director, Ken McDonald. It has been very much a part of seeing the CPS working in partnership much more closely with the police and much earlier in cases than was historically the case without letting go of our independence and continuing to respect the independence of the police, recognising that there is huge value in that partnership in delivering a better service.

Chairman: Thank you very much. May I thank all of you for your very helpful answers to our questions? You will be sent a transcript to check that you are accurately recorded and if, on reading the transcript or indeed even before, you think there are things which it would be helpful for us to have in writing please feel free to let us have them. Thank you very much indeed.

WEDNESDAY 22 NOVEMBER 2006

Present	Avebury, L	Dubs, L
	Bonham-Carter of Yarnbury, B	Harrison, L
	Caithness, E	Henig, B
	Corbett of Castle Vale, L	Marlesford, L
	D'Souza, B	Teverson, L
		Wright of Richmond, L (Chairman)

Memorandum by Baroness Ashton, Parliamentary Under-Secretary of State, Department for Constitutional Affairs

CO-OPERATION BETWEEN THE NATIONAL SUPERVISORY AUTHORITIES AND THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

1. Provisions for co-operation between the national supervisory authorities and the EDPS are found in Article 53B of the Decision.[1] The national supervisory authorities and the EDPS will provide co-ordinated supervision of SIS II and co-operate actively in the framework of their responsibilities via the methods below (as required):

- exchanging relevant information;
- assisting each other in carrying out audits and inspections;
- examining difficulties of interpretation or application of the Decision;
- studying problems with the exercise of independent supervision or in the exercise of the rights of the data subject;
- drawing up harmonised proposals for joint solutions to any problems; and
- promoting awareness of data protection rights.

2. The national supervisory authorities of the Member States will have responsibility for supervising the SIS II data protection regime at Member State level: this will be the Information Commissioner in the UK. The EDPS will monitor the personal data processing activities of the Management Authority in line with Articles 46 and 47 of Regulation 45/2001.[2]

3. The Decision sets out that national supervisory authorities and the EDPS will meet twice a year, with the costs and servicing of meetings met by the EDPS. Further working methods will be developed jointly according to need. A joint report of activities is to be prepared every two years and sent to the European Parliament, the Council and the Management Authority.

4. The national supervisory authorities of the Member States currently participating in the first generation SIS co-operate through the Joint Supervisory Authority arrangements. The ICO and the EDPS have links with other national supervisory authorities, for example, through the Data Protection Directive Working Party. This body has a number of tasks similar to those in SIS II such as the development of European standards and common interpretations, and promoting awareness of data protection measures.

5. The DCA and the Home Office are content with the provisions for co-operation between the national supervisory authorities and the EDPS with regard to SIS II.

MONITORING ACCESS, AUTHORISED PERSONNEL AND TRAINING

6. Member States must put stringent measures in place to ensure high levels of security and confidentiality. The requirements for monitoring access in Article 10 of the Decision[3] include facility access controls, user controls, and data access controls. For example, it must be possible to subsequently verify users accessing a system and the data processing they have carried out.

[1] There are equivalent provisions in Article 31B of the SIS II Regulation. The UK has opted out of participating in the immigration and border control measures covered by the Regulation, but is a full participant in the police and judicial co-operation measures covered by the Council Decision.

[2] Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community, institutions and bodies and on the free movement of such data.

[3] Article 10 of the Regulation.

7. Article 10 requires Member States to adopt security measures related to authorised personnel to (amongst other things):

- deny unauthorised persons access to data-processing facilities;
- prevent the use of automated data processing systems by unauthorised persons;
- ensure that persons authorised to use an automated data processing system only have access to the data covered by their access authorisation and with individual and unique user identities and confidential passwords only; and
- ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems; when; by whom; and for what purpose.

8. Article 10A[4] requires Member States to apply rules of professional secrecy or other equivalent obligations of confidentiality to all personnel required to work with SIS II data. These rules continue to apply after those staff transfer to a different area of work or change employer.

9. Every access to and all exchanges of data must be recorded in keeping with the requirements in Article 11[5] in order that the lawfulness of processing can be checked and security measures monitored. The records must show the data used to perform a search, the reference to the data transmitted, and the name of the competent authority and the person responsible for processing the data.

10. Member States must ensure that each authority adopts suitable measures to monitor their own compliance with the Decision (Article 11A[6]) and co-operates with the national supervisory authority.

11. Personnel must be given appropriate training on data security and data protection rules, and be informed of relevant criminal offences and penalties, before being authorised to process SIS II data (Article 11B[7]).

12. The measures in Article 10 are based on the data security measures in the Europol Convention. The Home Office has consulted DCA, SOCA and the Home Office SIS II Programme Team and no concerns have been expressed about the adequacy of these measures. A representative from the Joint Supervisory Authority (JSA), with responsibility for supervising data protection in SIS I+, attended the Schengen Acquis working group on 10 April 2006 and confirmed that the JSA, European Parliament and other interested parties were content with the data protection and security arrangements.

13. In addition to self monitoring and supervision by the national supervisory authority, Member States are evaluated before they may access SIS data as part of the Schengen evaluation process. A Schengen evaluation team conducts a data protection evaluation and checks that the necessary safeguards are in place in relation to access controls, authorised personnel and training.

14. Law enforcement access to SIS II data in the UK will be provided via a seamless link to the existing Police National Computer (PNC). All transactions on the PNC are logged and fully auditable thus ensuring that any search or update carried out on PNC/SIS II in the UK can be traced back to the originating member of staff. As noted above with regard to SIS II, the purpose for the transaction is also logged on the PNC.

15. The UK Sirene Bureau, located within SOCA, is the nominated agency responsible for SIS II management and security measures. SOCA will cooperate with the representatives of the operational users of SIS II (Joint Operational Authority, Sirene UK) to ensure that data protection and auditing responsibilities are agreed and published. The UK Sirene Bureau must also comply with applicable requirements in the UK Data Protection Act. The Information Commissioner's advice was sought at an early stage in the development of the UK Sirene Bureau. The Information Commissioner has the right to investigate the use of SIS II data by law enforcement agencies within the UK. In addition, the UK Sirene Bureau and the agencies using the system are subject to a peer review on a regular basis.

Europol and Eurojust

16. Article 37A of the Decision provides Europol with the right to access and search data entered into SIS II. Using the information obtained from a search is subject to the consent of the Member State concerned. The handling of such information is governed by the Europol Convention, should the relevant Member State consent to the use of the data obtained.

[4] Article 10A of the Regulation.
[5] Article 11 of the Regulation.
[6] Article 11A of the Regulation.
[7] Article 11B of the Regulation.

17. Additionally, Europol must:

- record every search in accordance with the record-keeping requirements set out in Article 11;
- not transfer, copy or download parts of SIS II;
- limit access to specifically authorised personnel;
- adopt measures for security and confidentiality noted in Article 10;
- allow the Joint Supervisory Body (set up by the Europol Convention) to review access to and searches of SIS II data; and
- only communicate such information to third states and third bodies with the consent of the Member State concerned.

18. Article 37B provides equivalent rights for Eurojust. The Council Decision establishing Eurojust includes provisions relating to data protection and unauthorised processing, and the powers of the Joint Supervisory Authority; these are not affected by the SIS II Decision.

19. Eurojust must comply with the same requirements set out in paragraph 17.

20. The rules regarding the use of SIS II data by Europol and Eurojust are detailed, specific and proportionate and both the Home Office and DCA are content that they will safeguard the security of shared data. No concerns about these rules have been raised by other Member States.

SIS II and the Data Protection Framework Decision (DPFD)

21. The DPFD will provide common standards of data protection in the third pillar (police and judicial co-operation) and will provide an overarching data protection framework for existing and future EU instruments concerning the exchange of personal data.

22. Articles 48A and 49 of the SIS II Decision require that personal data is protected in accordance with Convention 108 of the Council of Europe 1981 for the protection of individuals with regard to automatic processing of personal data.[8] When the DPFD is implemented references to Convention 108 in third pillar instruments, including SIS II, will be taken to refer to the DPFD (DPFD Article 34(2), Document 11547/3/06 REV 3).

23. The data protection principles in Convention 108 (and subsequently in the DPFD) are supplemented or clarified in the SIS II Decision where necessary.

24. Other existing protections that will apply to SIS II include:

- Council of Europe Recommendation No R(87)15 1987 (regulating the use of personal data in the police sector).
- Regulation (EC) No 45/2001 (processing of personal data by the Community institutions).
- Europol Convention 1995 (provisions concerning data protection apply to processing by Europol).
- Council Decision 2002/187/JHA 2002 (provisions concerning data protection apply to processing by Eurojust).[9]

25. Title VI of the Schengen Convention 1990 contains provisions regarding the protection of personal data communicated outside the Schengen Information System. Those provisions will not be amended by the SIS II Decision, but will be replaced by the DPFD with regard to matters falling within the scope of Title VI of the TEU.

4 October 2006

[8] The SIS II Regulation requires that personal data must be processed in accordance with the first pillar Data Protection Directive (95/46/EC).

[9] The DPFD will not apply to the processing and protection of personal data under the instruments relating to Europol and Eurojust.

22 November 2006

Examination of Witness

Witness: BARONESS ASHTON OF UPHOLLAND, a Member of the House, Parliamentary Under-Secretary of State, Department for Constitutional Affairs, examined.

Q248 ***Chairman:*** Baroness Ashton, thank you very much indeed for coming to answer our questions, and indeed to say whatever you want to say to us. Perhaps for the record I should say that this meeting is on the record, it is being broadcast and it is, as you know very well, part of our scrutiny into the Schengen Information System Mark II, I think known as Schengen II, is it not, now, so we can cut out a few of those words. May I thank you very much also for your written evidence, which you sent us on 4 October; that was extremely helpful. Would you like to say anything to start with?
Baroness Ashton of Upholland: On a slightly tangential point, I just wanted to say to the Committee that I am aware it has been difficult to organise diaries and I would not want there to be any impression given that I am in any way other than fully conversant with my responsibilities to Parliament and to this Committee. Indeed, I am heading for the Arctic Circle later on today to do a conference and I have actually altered my arrangements. I will fly out there in the middle of the night in order to be here. I know there have been some difficulties in trying to arrange it and I would not want the Committee, for one minute, to think that we are anything other than absolutely alive to my parliamentary responsibilities.

Q249 ***Chairman:*** It is very kind of you to say that. We are all very conscious of the pressures on your diary and are all the more appreciative of your readiness to come and give evidence to us today; so, again, welcome. Can I start off by asking you has the SIS II, Schengen II, legislation now been fully agreed between the Council and the European Parliament, including the data protection implications of access to SIS II data by the security services? At the risk perhaps of duplicating some of the points you have made to us in writing, can you explain what position the Government took on this issue and why?
Baroness Ashton of Upholland: Thank you, My Lord Chairman. The First Reading agreement has been reached between the European Parliament and the Council, which is good news. You will know that a huge amount of work on this has gone in from the UK side. There was an amendment put forward which was to allow access for all authorities which actually were entering data in SIS II, and of course in some Member States that would have provided access for security services. You know that we do not accept and do not believe that national security matters are covered in the third pillar. The amendment was not acceptable. The Government is quite comfortable with reverting to the position which exists, which is that Member States nominate those agencies which will have access to SIS II, regardless of whether they actually put information in. We are quite comfortable that we are in a good place on this and we look forward to what the Presidency will do now, in terms of taking that forward.

Q250 ***Chairman:*** Thank you very much. Is the Government content that the relationship between the Data Protection Framework Decision and SIS II Decision is spelt out sufficiently clearly in the texts? What is the current state of discussions on the Framework Decision, and what are the outstanding issues?
Baroness Ashton of Upholland: I am content that it is covered, My Lord Chairman. You will know that both in the SIS II document, in Article 50, and in the Article 34 in the Data Protection Framework Decision document, (a) it spells out very clearly in the data protection document that Convention 108, the references to that will be superseded by the references to the Data Protection Framework Decision, and that within Article 50 of the SIS II document there is the reference to in accordance with the law of the Member State before they invoke that right with access to the data. I am reasonably confident that has been done very effectively. As you know, the data protection document which will replace Convention 108 is the base set of arrangements around data protection. SIS II is a much more detailed, particular framework, which will apply, of course, in the particular contexts.

Q251 ***Lord Marlesford:*** Minister, can I raise a point which I think is of fairly overriding importance and the Committee has discussed with various people in the past. Here we are, entering SIS II, and we are all very concerned with the information, security, and all the rest of it, but the thing which is also concerning us is to find that because we are not "full members of Schengen" we are not getting access to the full information of the Schengen system. What is the Government's view of that denial of access and what will you do about it?
Baroness Ashton of Upholland: Inevitably, I tread cautiously and carefully into territory which is absolutely the responsibility of the Home Secretary and the Home Office. However, within the Justice and Home Affairs portfolio we work as a team, and certainly I have been party to conversations with the Commission to see whether it is possible to expand

and extend the way in which we operate. We do, of course, reserve and remain outside of large parts of the Schengen agreement, and alongside the agreement and membership of that agreement goes the ability to access all the information. There is a negotiation, I think, which is always ongoing, to see how far we can access information. Obviously, the purpose of all of this is to make sure that we tackle issues such as serious and organised crime effectively; there is no reluctance on behalf of other Member States or the Commission to see the UK participate in that. However, because we are outside Schengen *per se*, we do not have access and never will. This is something you may wish to pick up with the Home Office as well, because they will be far more up to date on their negotiations than obviously I am, because those were discussions during the Presidency and I have not had any subsequently.

Q252 ***Lord Avebury:*** The Minister was making a distinction in her first reply between the agencies that will have access to the SIS II information and those that can enter data, which will be, as we understand it, any law enforcement agency which is on a large list in the United Kingdom of some, I think, 80 different police forces and other law enforcement bodies. How will this large number of bodies make a distinction between their initial collection of data, which is governed, as we understand it, by domestic data protection law, and the cross-border exchange of that data, particularly the entry of the data into the SIS II System which is governed by the DPFD? As a supplementary to that, could I ask you why the Government objects to applying the DPFD to the domestic data protection issues?
Baroness Ashton of Upholland: There was an issue, Lord Avebury, very simply, about the legal base, which is still under discussion and negotiation, and inevitably we are cautious about doing anything which would imply that, because something is desirable, you can determine that the legal base is different from that which actually exists. That is the legality side of it. There is a pragmatic and practical side of it which goes alongside that. In looking at the data protection questions, I have met with all of the agencies which have been involved and they have raised, quite understandably, specific points of concern. These were notably that they did not wish to have two systems that were fundamentally very different from each other, not least because that could lead to mistakes or perhaps people not sharing information. They were pleased with the way in which our data protection work operates, or the Act operates, in that sense, and therefore were keen to see what happens with the European Framework, as much similarity as possible. I have taken those seriously on board and what we would look to do is, assuming that the legal base does not allow that this be moved into the third pillar, look at our own domestic legislation in order to make them match as far as possible. Ultimately, we want to make sure that the systems work, but we want the standards that we have here, and hence my officials, who have worked tirelessly on this for some months, have been working closely both with the European Parliament and the Commission and in the Working Groups to try to make sure that is as effective as possible. We are making good progress on that.

Q253 ***Lord Avebury:*** If we did have to alter our own Data Protection Act then that would have to be slotted into the legislation programme. Are you satisfied that you could reach agreement on this in time to go through all the procedures of giving instructions to Parliamentary Counsel and finding time within the legislative programme to do this before we enter SIS II?
Baroness Ashton of Upholland: SIS II is some way off, as you know. First of all, I do not know whether we will need to alter our legislation. Secondly, we will have to look at whether that is by primary or secondary legislation, if we do, and then we will look at what we need to do. I do not think actually we are into substantive changes at this stage. The fundamental point, which I am pleased to put on the record, is that we would look to make sure that we were not creating difficulties in this very important area for our services and to take on board the comments that they have made, quite rightly, about wanting a system which looks as close to the other as it can. The issue, in a sense, is that, if there is no legal basis to do that, we need to look at it pragmatically and we are committed to doing that, and I am happy to keep the Committee informed about that, because that is an area of interest as we move forward. At this stage, I do not know what, if anything, I need to do.

Q254 ***Lord Dubs:*** Why has the Government not opted in to the jurisdiction of the Court of Justice over third pillar issues? How often has this issue been reviewed and when will it be reviewed next, if at all? Would opting in not help to ensure a more consistent interpretation of third pillar measures and the protection of individuals' rights, for example, in the context of SIS II?
Baroness Ashton of Upholland: It is a big question for a small Data Protection Minister. The last time it was discussed was between the Constitutional Treaty discussions, and I understand that it will be looked at again in 2007, at the end of the period of reflection, I think it has been described as, when those issues will be looked at again. There are lots of issues, for example, workload, and so on, that I

know the European Court will have to think about. I cannot really say any more than that, at this stage, for it is not in my hands, other than to answer the question directly, which is that it will be looked at again at the end of the period of reflection, in 2007.
Chairman: Thank you for that answer to a big question.

Q255 ***Earl of Caithness:*** Minister, there seems to be a discrepancy between the SIS II and the DPFD as to the data subject's right of information. The DPFD does provide a right to be informed whether data is held on oneself, who controls that data and for what purpose it is held, and does the Government agree that such a right should apply to policing and criminal law, and SIS II in particular?
Baroness Ashton of Upholland: The quick answer to that is, yes, we do. It is quite interesting, because in Article 50, I think it is, in Schengen, it is the only place that I can see where, in a sense, the way that the Data Protection Framework Decision is looking, and within the documentation, it gives a kind of higher approach than elsewhere. The Data Protection Framework is generally the sort of base-line and then you have got, within Schengen, the ability to be more detailed and to have tighter restrictions. Actually, this is the one place where the Data Protection Framework Decision, I think, is stronger. What will happen, as you will know, is that once the Data Protection Framework Decision is finalised there then enters a period of discussion on all of the documentation and all of the other issues where data protection comes into play and, if I put it in the vernacular, what will trump what. This is an area where I am very happy for the Data Protection Framework Decision to trump Schengen, because we would want to see exactly the same things apply that we have already in our national law.

Q256 ***Earl of Caithness:*** Which document is going to win, at the end of the day; is it going to be the Schengen document or is it going to be the DPFD document which is going to override the other? Secondly, Minister, should not an awful lot of this have been thrashed out and explored before even we got into thinking about SIS II.
Baroness Ashton of Upholland: The answer to your question about override is that, in general, the Data Protection Framework Decision is the base-line of data protection which applies generally and there are specific tighter controls which generally would override that, because they are better and stronger and people feel more confident with them. As a generality, the Schengen controls are better than the Data Protection Framework Decision ever will be, because they are very specific, not because it is not good but they are very specific. This is the only one where I think the Data Protection Framework Decision, as it stands currently, is better. The negotiations and discussions about what trumps what and what overrides what can happen only when we have finally got agreement on the Framework Decision, because, obviously, different Member States are worried about different aspects of it, the Parliament will have its say too, and we will end up, I trust, with a very good document as soon as we possibly can, and a very good agreement, and then those negotiations take place. I understand your concern that we hurtle down the road and end up where we are without those previous discussions taking place, but actually, in the context that the working groups are into the very detailed part of the discussions on Data Protection Framework Decision, and because we know a great deal about what is being proposed in Schengen, I do not think you need to worry about it. I think what we will discover is that, the Schengen Information System, the SIS II proposals on data protection are strong, the Data Protection Framework Decision will be a very good, sound base, and it will be these individual bits of discussion, not least around this, where the decisions will be made on what will work best and which are better. From our perspective, we think this is one which data protection should override.

Q257 ***Baroness D'Souza:*** Minister, your officials suggested that the Commission would make recommendations for harmonised standards on data collection, but the SIS II Decision appears to provide for the Commission to adopt binding rules. Could you say which will prevail?
Baroness Ashton of Upholland: The Commission are going to, as you know, make reporting and recommendations on what they think should happen. I think what my officials were, I will not say 'trying to say' because I am not entirely sure, I read the transcript but I cannot remember exactly what they said, we think, but we do not know, that they may well propose minimum standards, but at this stage we do not know what the Commission itself is going to propose; that is where I think they were more likely to end up.

Q258 ***Lord Dubs:*** Your officials suggested that a further decision would be necessary as regards 'one-to-many' searching of biometric data on the SIS, but the SIS II Decision appears to state that such searches will be approved automatically following a Commission report on the available technology. Which of the two is correct?
Baroness Ashton of Upholland: My officials are completely right, as always; there is no question but it is exactly as they said. It is the difference between identification and verification, which I am sure you

have discussed, and no doubt we will discuss with colleagues from the Home Office. What will happen is that the Commission will make a report; they are looking at the technology to see whether it is appropriate and ready; they will put that report to the Council. There would need to be a unanimous decision to take that forward, if it was to go forward in that way.

Q259 ***Baroness Henig:*** I understand that the forthcoming German Presidency intends to propose that the Prüm Convention will apply to all Member States as an EU measure. Does the UK support this and would there then be a conflict between the data protection provisions of the Prüm Convention, on the one hand, and those of the DPFD and SIS II, on the other?
Baroness Ashton of Upholland: The provisions within Prüm allow for the national legislation to apply, so there would not be a conflict in that sense, our national legislation would apply, the Data Protection Framework Decision would apply in Europe and, as I have said, there then has to be a way of looking at it from a national and a European perspective, to see that they tie in appropriately. The UK is not a member of the Prüm Convention, as you know. Discussions are underway because Prüm has much to offer, I think. I think in this Committee we have talked before about the different groupings which enable Member States to work together in particular ways and then hopefully to take that experience further when it is appropriate. Again, it will be for the Home Secretary to take this forward, but I know he will have areas that he will want to look at very carefully before taking us anywhere into the Convention, but it will certainly be in discussion.

Q260 ***Baroness Henig:*** So cautious support for the process?
Baroness Ashton of Upholland: I think the Prüm Convention has so much to offer; there is a lot, in terms of looking at areas, for example, like serious and organised crime and the ability to work more speedily, but that brings with it other issues as well. I am sure the Home Secretary will want to do that but is interested in talking to them, which is the right way.

Q261 ***Lord Teverson:*** Minister, I am interested to know whether the Government welcomed the fact that six other Member States went off and tried to move ahead of the rest of the EU, and does the Government see this as coercion to the rest to move forward, or does it work in diversity within the EU?
Baroness Ashton of Upholland: It may be a Government view; it is actually a personal Government view, in the sense that within the 25 Member States there were groupings of Member States who had worked collaboratively in different ways. I think the example I gave last time, from my own area, is that we have a small group of countries—Malta, Cyprus, Ireland and ourselves—who have formed the Common Law Club, and our purposes, led by the Lord Chancellor, are specifically to look at proposals which come out of the European Union from a common law viewpoint, which is, as you know, in a minority. Although we may disagree on policy and it in no way binds anybody, we do find it useful to be able to think about issues, because the common law brings with it challenges when you are trying to develop across 25 nations. It is a very different kind of example, but nonetheless it is an example where working together collaboratively as a particular group is of benefit. I am not at all surprised that, within a group of 25 nations, who work, I think, remarkably well together within the Justice and Home Affairs Council, groupings which are facing particular issues or which traditionally work together in particular ways want to come together. I do not see anything difficult about that. I think it is interesting that the German Presidency, and I have not seen any information on this, but if it is correct that they are looking at what this might mean I am sure that the Justice Minister will bring that forward and discuss it at the informal and with colleagues, as appropriate. I see nothing wrong with that at all; far from it. It may be a way of actually testing out and looking at ideas before they are put across the 25 nations.

Q262 ***Lord Avebury:*** We understood that your officials were content with the rules governing access by Europol and Eurojust to SIS II data, but I wonder if you could tell us how you think those rules could be enforced, bearing in mind that they are not justiciable in the courts of either the Member States or the ECJ?
Baroness Ashton of Upholland: I was quite taken with this question because it is not an area that personally I have looked at in great detail, so if I can just express gratitude, because it is always useful to have the opportunity to look again. I know that obviously the supervisory bodies are very important, and you heard from the Information Commissioner's office, and David Smith's role within Europol is very important in that. Having looked at it, I think I am reasonably satisfied that there is a way forward, because the way that the supervisory bodies operate is that they are receiving information on a regular basis about what is happening within the bodies themselves, they are able to call to account and ask for information and demand it within reasonable timescales. Although you always hope that the bodies will work collaboratively within supervising the work of an agency, I think they have got quite a lot of informal

clout, I would not say that it is so much formal powers, to be able to hold to account. That feels all right to me but I am grateful for having had the chance to look at it, and in fact I was going to talk to David Smith about it separately, because this is something that, I think, in his evidence to you, is an area that is obviously of particular interest to him.

Q263 ***Earl of Caithness:*** Minister, you said they could be called to account; who can call them to account?
Baroness Ashton of Upholland: The supervisory bodies are able to say to the Director of either agency that they wish to have information within a timescale and require them to do it. They would then report on that, either back to their Member States or to the Commission or to the Council. It is not a power in the sense that we would traditionally describe it; however, it does seem to give them the right kind of leverage to be able to ask the question and to expect to be given the information, and to be able to push that forward if that were necessary. That feels, for these particular organisations, at the moment all right, but, as I say, I am grateful because I had not looked in detail at what the powers were until the Committee asked me the question.

Q264 ***Lord Avebury:*** I suppose there is a remote possibility that the supervisory body could ask Europol or Eurojust to do something and there would be disagreement on it, which would then be irresolvable because there would be no court to which the supervisory body could apply either. Do you not think that there should be some sort of last resort procedure for dealing with any difference of opinion which may occur between the supervisory bodies and Europol or Eurojust respectively?
Baroness Ashton of Upholland: I do not see it as a relationship which, in a sense, brings in the court. The way that they operate is that they can call it to the attention of the management board, they can ask for information, it is accepted that the information would be available; if it were not available the supervisory body could go to the management board and through them to the Member States, to the Commission, to the Council, wherever they wanted to go. I do not think that you need to have the power of the courts behind it *per se*, because I think the way that it is established as an entity the supervisory body actually is able to make requests, because that is what it is there for, and this is expected, that they will respond. In other words, it is part of the management contract, in a sense, between them. That is not unusual in lots and lots of organisations and institutions. I do not think necessarily you need the management board to be able to go to court if it does not get it, because the management board can simply go to the Member States or to the Council. I think it is all right. It is an interesting area, but I think, the way that they have done it and the way in which the opportunity to question is established, that it feels as if they do have the right kind of inquiring power without needing to have that in a legal framework.

Q265 ***Chairman:*** Minister, it is good of you to say that you welcomed, I think you said you were taken by, these questions. If later, and this applies of course to any of our other questions, having looked into this further, you wanted to send us any supplementary note, we would of course be very happy to receive it?
Baroness Ashton of Upholland: I would be delighted to do that. I am genuinely grateful for that.

Q266 ***Lord Marlesford:*** Minister, there has been some concern expressed, not least by the Commission, that there are not sufficient resources to implement the data protection provision properly. Would you like to comment on that both from a UK perspective and perhaps as far as that of other countries in the system?
Baroness Ashton of Upholland: I think David Smith said in his oral evidence to you, on behalf of the Commission, that there was an issue in other parts of Europe. I am afraid that is beyond my competence to know. Certainly he would have and the Information Commissioner, Richard Thomas, would have a greater understanding of the resource implications for the States. As far as we are concerned, domestically, and again I always make sure that I check the latest position, the Information Commissioner has been very clear that in the domestic sense what he has is adequate for his purposes, and to my knowledge that is the position as it stands currently. Again, what was interesting, I think, about the evidence that Mr Smith gave to you was him talking about the role that he is playing now within Europe and the implications of that, and certainly, as he will know, if there are issues that he wants to raise with me around that I would be more than happy to discuss them with him; but there are none so far, so, so far, so good.

Q267 ***Baroness Bonham-Carter of Yarnbury:*** We heard from the Deputy Information Commissioner, in evidence which he gave to us, that his office, and he put it rather discreetly, I think, was excluded to some extent from the negotiation on third pillar data protection measures. Considering the experience of that office, why do you think this is happening, and would it not be better to include them more?
Baroness Ashton of Upholland: I think he said also that I was very clear that I wanted to work very closely with the Information Commissioner's office in developing that. I do not think we have got that quite right yet, would be my response. There are a number of constraints under which we operate. The first is, we

cannot release documentation which gives the position of Member States, it is forbidden, because the negotiations are confidential, so we cannot send anything, and that means, if you like, we have to doctor the documents in order to be able to give a full account. We need to think about how we do that more effectively to give more information. When we ask some for information we do not get it, quite often, and I think we have got some work to do on establishing the most appropriate way in which we involve them. For my part, I agree with you, it is absolutely essential that we involve them appropriately in this, because (a) they have expertise, and (b) what they feel and think about this will be very important in the future, and I do not want to lose that experience or expertise by accident. My response is I have asked officials to have a think with them about how we make this work better than it does now, because clearly it is not working as well as it might, from either end, and hopefully they will resolve that to our satisfaction. I am more than happy to come back and explain what we did. It is not anything other than trying to get the administrative side of that to work effectively; it is not other than the desire to make it work well.

Q268 ***Chairman:*** Minister, I quite understand the problems, but I think I should record, throughout this scrutiny, a very strong feeling in this Committee that the closer your Department can work, and indeed the Home Office can work, with the Information Commissioner the happier we will be.
Baroness Ashton of Upholland: I accept that.

Q269 ***Chairman:*** I am sorry, that is perhaps a statement of the blindingly obvious?
Baroness Ashton of Upholland: No. I accept that. I have lots of responsibilities myself, including for the Information Commission, and I do work very closely with a range of different things. Getting the processes right, as you will know, Chairman, is sometimes more difficult than at first it looks; and clearly we have not quite managed this, but that is not lack of desire, it is just trying to get it set up properly.
Chairman: I quite understand.

Q270 ***Lord Harrison:*** Minister, I am a new member of this Committee but I am speed-reading, very quickly, all that is presented to me. Because the Government has absented itself from the Schengen system, as I understand it, therefore, in terms of the Information System, both the current one and the one which is proposed, again we absent ourselves from access to information which might be very useful indeed to the United Kingdom. I understand some of the practical questions that you raise and political questions, concerns about the data protection, but has anyone, either in the DCA or indeed in the Home Office, done an analysis of what we would lose by being absent; in other words, turned it on its head and said, "Well, these are the areas that might be very useful to us"? Indeed, there may have been practical examples of where we would have liked to have access to important information for the purposes of the defence and security of the United Kingdom?
Baroness Ashton of Upholland: As I think I was partly explaining, in answer to Lord Marlesford's question, these are issues obviously to pick up with the Home Office directly. I do not know if they have done a detailed analysis but certainly I know that they have considered areas where greater access could be of benefit. I think, as I was indicating, during our Presidency there were discussions about whether we might be able to access more information. As I have said already, membership of Schengen carries with it certain things; if you are not Schengen then you do not automatically get the right to participate in that. That is a bigger and more political and strategic issue, and definitely for the Home Office and certainly not for me, but I think I can say that they are very alive to the issues and concerns there will be. Of course, you are absolutely right that the critical factor in all this is what we need to do to make sure that we keep people as safe as possible and tackle issues of serious and organised crime.

Q271 ***Lord Avebury:*** Do you not think it is incongruous for the Commission to have delegated work on the Data Protection Framework Decision to a body which is called the Multidisciplinary Group on Organised Crime? It is not simply the Information Commissioner who is excluded from knowledge of what is happening in this black hole but the whole of the public in the European Union. Do you not consider that it is unsatisfactory that we should know so little about the processes by which agreement is reached on the DPFD?
Baroness Ashton of Upholland: The Multidisciplinary Working Group is the same as any other working group, it has just got this name, because it is when they are tackling issues to do with serious and organised crime they come together under that name. When they are discussing data protection, it is the DCA officials who attend it, so it changes, under its name, into all of the officials from across the European Union dealing with data protection. There is always a difficulty, when the working groups are meeting and the detailed negotiations are going on, about confidentiality, it is one of the things which on occasion are of great benefit, because the quality of the discussion occasionally can be enhanced, if you are actually being able to talk in the right kind of detail. That is one of the issues about the documentation which comes out of the working group not being spread around, so people are not

seeing precisely where nations are sitting at any one particular moment. Certainly from the UK perspective, in detailed negotiations, we have found that very valuable. I am in the privileged position that I do get reports of what is happening and my officials are deeply involved in what is occurring, so that I can be happy in thinking that we are making good progress. Just to say that, of course, this was an area which I undertook that the UK would participate in very, very fully during our Presidency, in order to make sure that these safeguards were done as well as possibly they could be, and we have supported the Finnish Presidency and we will support the German Presidency in doing that.

Chairman: Minister, thank you very much indeed for coming today, and particularly warm thanks for your very helpful and frank replies to our questions, even to our big questions.

MONDAY 27 NOVEMBER 2006

Present	Avebury, L	Henig, B
	Bonham-Carter of Yarnbury, B	Listowel, E
	Caithness, E	Teverson, L
	Dubs, L	Wright of Richmond, L (Chairman)

Examination of Witness

Witness: Dr Wolfgang von Pommer Esche, Head of Unit, Police Intelligence Service, Federal Data Protection Office, Bonn, examined.

Q272 ***Chairman:*** Can I first ask you how I should address you. You are Dr von Pommer Esche, is that right?
Dr von Pommer Esche: That is right, but I am not a doctor of medicine, I am a lawyer.
Lord Dubs: Still "doctor".

Q273 ***Chairman:*** Absolutely. In fact, a lot of doctors and lawyers in Germany are "doctor doctor", are they not?
Dr von Pommer Esche: Doctor doctor, doctor of law and doctor of economics.

Q274 ***Chairman:*** That is right. Anyway, Dr von Pommer Esche, thank you very much indeed for coming to give evidence to us. As you know, this inquiry is an inquiry by a Lords sub-committee into Schengen II, the Schengen Information System Mark II. It is on the record, although if at any point you want to go off the record that is perfectly acceptable to us, otherwise a full transcript is indeed at this moment being taken of this meeting. You will be sent the transcript in due course and it is entirely up to you to say whether you are content with the remarks attributed to you.
Dr von Pommer Esche: Yes.

Q275 ***Chairman:*** Welcome, and thank you very much for coming to give evidence to us, it is extremely useful. I think you have probably had notice of our questions.
Dr von Pommer Esche: Yes.

Q276 ***Chairman:*** The first question I really want to put to you is what can you tell us about the extent to which national supervisory authorities are enforcing SIS data protection provisions, how far are individuals able to enforce these provisions and, perhaps most particularly, what is your experience in your own country in Germany?
Dr von Pommer Esche: Thank you for that question. I come from the office of the Federal Data Protection Commissioner. I am head of the unit responsible for compliance with data protection rules for the German Federal Police Forces, for the German Secret Service, for security screening and for police and judicial co-operation in Europe. I have been in office now for about 16 years, that means for a very long time. Shortly after the signing of the Schengen Implementation Agreement I started my present function.

Q277 ***Chairman:*** I spent most of my diplomatic life in the Middle East and when somebody tells you that he has been in the same job for 16 years, you say in Arabic "May God give you rest"!
Dr von Pommer Esche: We are not as flexible in our office, myself and my colleagues,as in the Ministry of the Interior. All heads of unit come from the Ministry of Interior.

Q278 ***Chairman:*** Can you give us any idea of enforcement, the extent to which national authorities or individuals are—
Dr von Pommer Esche: As the Federal Data Protection Commissioner we have competence for the supervision or the monitoring of data processing, which is at federal criminal agency, *Bundes Kriminalamt.* The *BundesKriminalamt* is the central body for Schengen according to Article 108 of the agreement. In that capacity we get requests for information from individuals. In Germany there are two ways to exercise this right. An individual can directly address the controller of the file, that means the greater part of the requests are directed to the Federal Criminal Agency, but we also receive requests for information, especially from other European colleagues, for instance from France, or we receive requests in cases where an alien has not got a *visum*, i.e. it has been denied due to certain security reasons. There is a special procedure with Schengen according to Article 17, paragraph 2 of the Convention. If you are a *visum* applicant from certain states with a terrorist background then you have to undergo this procedure and your request is checked against the data files of the security services. We sometimes receive requests in those cases. We receive about 30 or 40 requests for information per year in the case of Schengen.

Q279 ***Chairman:*** Do you have any views on the process of negotiating Schengen II? Were your national data protection authorities involved, and involved sufficiently in your view?
Dr von Pommer Esche: Yes. We are involved both via the international flow, via Brussels, via the Schengen Supervisory Authority and also involved via our German channels, I would say. In Germany it is the case that there are rules of procedure of the Federal Government and when the Federal Government deals with matters, bills and so on, which have any kind of data protection implications then we have to be involved. We are well-informed about these kinds of bills or projects.

Q280 ***Chairman:*** The same is true of the Data Framework Directive and negotiation of SIS II?
Dr von Pommer Esche: Yes.

Q281 ***Chairman:*** Good. Thank you very much.
Dr von Pommer Esche: We get papers and papers. It is only a question of the capacity to cope with all of these papers. In my unit there are only five of us.
Chairman: I can understand the problem.

Q282 ***Lord Avebury:*** Within your knowledge of the regimes of data protection in other Member States, do you consider that they all have sufficient resources to carry out the tasks that are expected of them under the current SIS rules and also under the SIS II legislation?
Dr von Pommer Esche: I am not informed about the state of knowledge in other countries but I have got the impression via discussions with my colleagues in other countries that in most cases in Germany we are better informed than my colleagues in other countries, although the government is in Berlin and we are still in Bonn and that means we are 550 kilometres from the government. Maybe you have heard about the Prüm Treaty. I had the impression from some colleagues that they were not at all informed about the negotiations of such a far-reaching Treaty or far-reaching project like the Treaty of Prüm.

Q283 ***Baroness Bonham-Carter of Yarnbury:*** Can I ask you about access to data. I believe that the Commission have proposed detailed new rules on access and the Austrian Presidency has proposed instead simply retaining the Schengen Convention. In your opinion, is the SIS II legislation sufficiently precise as regards which authorities can access data and for what purpose data can be used? Does the third pillar SIS II decision sufficiently limit the purpose for which data can be used?
Dr von Pommer Esche: Thank you for that question. In principle I would say that the legislation or the proposals are clear enough with one exception: at the end of the negotiations in September/October there was a question as to whether the secret services shall have access to the SIS, not to all kinds of data but to certain alerts, and I found the wording of that clause in the proposals very tricky. It was very difficult to understand what was behind this wording. It has not been denied. It was approved by the Council but the Parliament was against the inclusion of the secret services to get access.

Q284 ***Baroness Bonham-Carter of Yarnbury:*** Are you concerned about the possible access to data for asylum purposes?
Dr von Pommer Esche: By which authorities?

Q285 ***Baroness Bonham-Carter of Yarnbury:*** By any authorities. Are there sufficient safeguards, I suppose is what I am asking you.
Dr von Pommer Esche: The access to the immigration data is regulated in Article 17 of the draft Regulation. As far as there is a reference to other EU or EC regulations, I do not find it very clear to define the competent authorities by reference to other regulations. On the other hand, I must say in the first draft, in the first version of the Regulation, it was still open as to whether other authorities will have access to this data and the police forces also. I think that these possibilities have been deleted.

Q286 ***Earl of Caithness:*** Doctor, is the relationship between the general data protection rules in EU legislation, that is the 1995 Directive and the proposed Framework Decision, and the SIS II legislation sufficiently clear in your view?
Dr von Pommer Esche: That was one of the key questions when we discussed these proposals in the different bodies. There are several regulations or several provisions to be taken into account. As basic regulations we have the Directive of 1995 for the first pillar, then we have the project of a Framework Decision on third pillar data protection, then we have the two SIS regulations and we have Regulation 45/2001. In Germany we have a data protection regime of general law and of specific law. We have a federal Data Protection Act with general regulations which is applicable unless there are specific rules. In Germany we do not have problems with this competition between different rules. As far as a matter is regulated, and exhaustively regulated, in a specific act this specific act prevails. The general act is only applicable insofar as there are no specific regulations. In the field of the EC and EU Law we feel that will have the same relationship with competition. There are some problems, for instance as regards the right of access and the right to information. So far in the draft Framework Decision on data protection there is a right of access and a right to information whereas, as far as I know, in the

SIS II decision there is no right to information, so the question arises if there is no right to information in the specific legislation. Is the right to information in the general rule, that means in the Framework Decision or data protection third pillar, applicable or not? From my point of view I would say although there is no regulation on the right to information in SIS II, there is the intention of the legislator that there should not be a right to information in the field of Schengen. That means the general rule cannot replace the missing regulation in the SIS decision. That is my opinion.

Q287 ***Earl of Caithness:*** Do you think your view is the majority view? Do you think that is how it will be interpreted?
Dr von Pommer Esche: I have not had any discussions with other colleagues. I have read your questions and I have thought about the problems. We have discussed these problems in general and dealt with them in the opinions of the Article 29 Group and in the Schengen JSA but we did not go so far into the details.

Q288 ***Lord Dubs:*** I think my question has largely been answered but if there is anything left to answer I will give you the opportunity. My question is this: how would you assess the current state of negotiations on the Framework Decision on data protection? To what extent would the Framework Decision, in the latest available text, affect the standard of data protection provided for in the SIS II decision, for example as regards a right to information? I think you have dealt with a lot of that.
Dr von Pommer Esche: As for the state of discussion on the Framework Decision, I find it disappointing. The Member States in the MDG have brought themselves to a negotiation situation where it is difficult to find a way out.

Q289 ***Chairman:*** Are you talking about the Council or the—
Dr von Pommer Esche: The Framework Decision on data protection is discussed in the Council and in the Parliament.

Q290 ***Lord Avebury:*** Do you have access to any of the working papers of the MDG? How do you know what is going on there?
Dr von Pommer Esche: I do not have all the papers which are tabled in the MDG but for each meeting the Federal Government prepares a joint position for further discussions in the MDG and in other Council working groups. As far as data protection legislation or questions are concerned, we are involved in most cases. I do not have any comments on that because I am outside the Federal Government.

Q291 ***Baroness Henig:*** Do you believe that the United Kingdom should have access to immigration data, at least for some purposes, such as asylum, or at least to come categories of that data, such as persons who are listed because they have committed criminal offences or are believed to have committed, or to be intending to commit, such offences?
Dr von Pommer Esche: I do not know whether you want to hear this or not, but my opinion is that the United Kingdom Government should not get access to the immigration data because the file with immigration data is a collection that for me is a compensatory mechanism for the abolition of the border controls. As the United Kingdom is insisting on the border controls I would find it out of proportion if the United Kingdom got access to this data for whatever purpose.

Q292 ***Baroness Henig:*** So is this quite a principled response from you?
Dr von Pommer Esche: Yes, for me it is a principled question.

Q293 ***Baroness Henig:*** So you would not take a pragmatic view that—
Dr von Pommer Esche: In that case I would say that this is not an official opinion of the Data Protection Committee, it is my opinion.

Q294 ***Baroness Henig:*** Can I just ask how widely shared is your opinion, do you think?
Dr von Pommer Esche: How wide is it?

Q295 ***Baroness Henig:*** Yes. If we talked to a cross-section of people who hold important positions such as you, would that be a general view do you think?
Dr von Pommer Esche: I have not had an exchange of views with the Federal Government, so it is not in discussion.

Q296 ***Baroness Henig:*** I meant people within the EU, people who are perhaps holding positions as you are, not necessarily German but other nationalities. I just wondered whether there were many of you who had discussed this and come to that view.
Dr von Pommer Esche: We discussed the access of the United Kingdom to the Schengen data files but that was years ago. I do not remember the details.

Q297 ***Lord Dubs:*** I understand, of course, that if the United Kingdom is not prepared to join Schengen then we should not get the benefits of Schengen membership. I think that is clear and I would not argue with that. However, it seems to me that some of the immigration data, because of the fact that international criminals and terrorists frequently cross borders, is important in dealing with criminal activity. Is there not a loss of information to the

Schengen countries through not having the UK's information and similarly there is a loss of information for the UK in not having the Schengen countries' information as part of the build-up of dealing with criminal activity?
Dr von Pommer Esche: I am aware that the United Kingdom is one of the favourite targets of asylum seekers and refugees from third countries and it is clear that international criminality and cross-border terrorism is without frontiers, it is a worldwide danger, but how will you limit or restrain the access of the United Kingdom for what purposes or for which criminal acts and so on? You must find a definition of "international terrorism".

Q298 ***Chairman:*** Of course, it is not for us to defend the British Government's decisions in this matter. To some extent the position of the United Kingdom, and indeed the position of Ireland, is a factor of our geography, would you not agree? We do not have either the benefits, or perhaps the disbenefits, of Germany. I cannot remember how many borders you have but you have got a very large number. I think you have more than any other member of the EU, do you not?
Dr von Pommer Esche: Yes, I think so.

Q299 ***Earl of Listowel:*** Doctor, does the SIS II legislation provide sufficient safeguards in respect of the biometric data and, if not, what should those safeguards be?
Dr von Pommer Esche: In the course of the negotiations the regulations have been improved. For a long time it has been crucial whether the biometric data should or should not be used in the SIS but now it has been decided that the biometric data, that means photographs and fingerprints, shall be used as features in the SIS. For me it is understandable that biometric data are used for a better identification and for reliable and fast identification on the borders. The use of these biometric data and their involvement is now regulated in Article 14a(c) of the regulation of both proposals. At the moment the purpose of their use is to make one-to-one searches. From my point of view, I do not have great objections to that method but if you look at Article 14a(c), paragraph three, there is an opening clause that in the long run these biometric data should also be used for one-to-many searches. That means in that case if the Schengen Information System was not used for control purposes only, it would change its character to a kind of investigative tool or method. That would be a new quality and in the long run if Member States insist on that possibility, which I cannot exclude, then we must reconsider additional safeguards. The use of biometrics is combined with some risks, it is not 100 per cent sure, and if you test the different methods of biometric features you have high false rejection rates. That means at the moment the methods are not reliable enough but the technique is going on and the methods will be better and better in the future.

Q300 ***Chairman:*** Can I ask, in your German identity card system are you now already applying biometrics?
Dr von Pommer Esche: The photo is on there and we are on the way to introducing fingerprints via the EU legislation. That was a very crucial point. It is as a result of the anti-terrorism discussion in our country that we will introduce it.

Q301 ***Lord Teverson:*** Are the provisions in the final SIS II Immigration Regulation on the right to information sufficient, and also any remedies?
Dr von Pommer Esche: The right to information is only regulated in the Regulation, not in the decision. I would say in Article 29 of the Regulation in paragraph one there is a reference made to the corresponding regulations in the Directive but in paragraph two there are far-reaching exemptions, so the question arises whether this right to information in practice will be of any value for the data subjects.

Q302 ***Lord Teverson:*** I take it from the way you have expressed that that your feeling is it is not satisfactory?
Dr von Pommer Esche: Yes. The exceptions, exemptions, I do not know exactly the right word—
Lord Teverson: For my benefit, could you remind me of the exceptions?
Chairman: As an example.

Q303 ***Lord Teverson:*** Under headings, briefly, which you think particularly make this an unsatisfactory exercise?
Dr von Pommer Esche: I am looking for the English version. This is the German version: "This information will not be given or if personal data has not been collected from the data subject", okay, I can understand that, "if the information to the data subject is impossible or an unreasonable amount of work is necessary."

Q304 ***Lord Teverson:*** Yes, yes.
Dr von Pommer Esche: "If the third state's national has already got the information or if, according to domestic law, a restriction to this right to information is provided for, especially for reasons of national security" and so on. In most cases, that is the case.

Q305 ***Chairman:*** Dr von Pommer Esche, can I just tell you that I have the English text in front of me and your translation is perfect.

Dr von Pommer Esche: Nearly perfect!

Q306 ***Lord Avebury:*** Can I ask you a more general question, which is whether you think that there are any specific provisions in the SIS II text or the SIRENE manual which need to be changed? Maybe you would want to take notice of that and let us have a written answer rather than running through the whole gamut of alterations that you would like to see if the alterations that you would envisage are at all extensive.
Dr von Pommer Esche: I would say as for the access to the immigration data, entitled authorities are authorities competent for border controls but also other police and customs authorities for making their checks. This enlargement, the second possibility, was not foreseen in the first draft of the SIS II Regulations. I would say this was a consequent approach of the Commission but in the course of the negotiations Member States have insisted that the normal police forces should have access to this immigration data, but in my view that is going too far.

Q307 ***Lord Avebury:*** I wonder if you have looked at the report by the European Parliament rapporteur which details a number of amendments that he would like to see in the text. I wondered, if you have had an opportunity of considering those, whether you have any opinion on them.
Dr von Pommer Esche: To be quite frank, I receive so many documents every day that I cannot cope with all these documents, it is too much.

Q308 ***Lord Dubs:*** I think we understand that.
Dr von Pommer Esche: Every morning I open my computer and there is a full range of documents. It seems to be a short document but then there are all the attachments, it is awful.
Chairman: Dr von Pommer Esche, I think on behalf of our Committee I should apologise for having added to your documents.

Q309 ***Baroness Bonham-Carter of Yarnbury:*** It has been decided that the Commission will not run SIS II but an agency. Do you have any concerns about the accountability of this future agency and, indeed, the French and Austrian authorities who are running it in the meantime?
Dr von Pommer Esche: I am not sure whether that is a data protection matter. We have been dealing with the Schengen System since 1995 and at the moment it is in the competence of the Member States but it is managed by the French Republic. I have participated in some information and control visits to Strasbourg and I have not seen any problems arising from France's special role. I do not see greater problems if SIS II were managed under the auspices of the Commission via a special agency alone.

Q310 ***Earl of Caithness:*** Doctor, do you think that the Data Protection Directive should be a model for the Framework Decision on Data Protection?
Dr von Pommer Esche: There are several resolutions and recommendations of the European Data Protection Conference. It is also mentioned in the statement of the Schengen JSA and the statement or opinion of Mr Hustinx of the EDPS. We should not invent a new kind of data protection for third pillar matters because that is confusing for the user and it is especially confusing for data subjects, for European citizens. If we need a third pillar mechanism, data protection mechanism, we should stick as closely as possible to the provisions of the Directive. It is clear that the Directive is applicable to the non-public sector. The relationships between the data processing bodies and citizens in the private field are mainly based on treaties, on contracts, whereas in the public field there is a relationship of highest and lowest, the highest are the public bodies and lowest the citizens, which is another relationship. We cannot use the regulations of the Directive one-to-one in the field of the third pillar but as far as possible we should use them for the rights of the citizens.

Q311 ***Earl of Caithness:*** Can I follow that up? Do you think that the Schengen II System is making data protection more difficult and is it adversely affecting the individual in comparison with the present situation?
Dr von Pommer Esche: The difficulty perhaps is that in future we will have two or three acts. We will have the decision and two regulations. We will have three models. At the moment we have the Schengen Implementation Convention and the regulations dealing with data protection in the SIS are Articles 92 to 119 for dealing directly with the SIS, and in addition we have the regulations of Articles 126 to 130 that are the data protection rules outside the SIS. The latter will be replaced by the Framework Decision on Data Protection and Articles 92 to 119 will be replaced by the Framework Decision on SIS II and Framework Regulations on SIS II. Maybe in the future it will be clearer than it is now. I hope so.

Q312 ***Lord Dubs:*** The forthcoming German Presidency is planning to propose that the Treaty of Prüm becomes part of EU law. Would this have any implications for SIS II and the related data protection regime? Could I ask you an additional question as part of that. Do you have a personal view on whether seven Member States should agree together and then impose their agreement on the other Member States? Perhaps that second question is a bit remote from the first one.

Dr von Pommer Esche: Thank you for that question. Ten days ago I was at a symposium in Vienna to promote the Treaty of Prüm and my task was to make a speech on the data protection aspects of that Treaty. I have heard that it could be an objective of Germany to make the Treaty into an EU instrument but it seems to me that is not simple to realise because the Prüm Treaty deals with first and third pillar material so you must create several legal acts. It seemed to me rather complicated. As to your second question, at the moment there are seven signatory states and in Vienna it was said that four other EU Member States are very interested in acceding to the Treaty, that would be Italy, Slovenia, Finland and Portugal, so maybe in the course of next year there will be 11 states, but it is still the minority of the EU.

Q313 ***Chairman:*** Do you have a text of your speech? Is it public? Do you have a copy of your speech at the seminar?
Dr von Pommer Esche: The speech is part of the documentation but it is in German.

Q314 ***Chairman:*** But it is a public document.
Dr von Pommer Esche: I made this speech in Vienna so I spoke in German.

Q315 ***Chairman:*** Of course, but it is a public document.
Dr von Pommer Esche: You can ask.

Q316 ***Chairman:*** Can I ask you to consider whether it would be helpful for us to see the text of your speech because it seems to me that a German view on this would be extremely helpful.
Dr von Pommer Esche: The Treaty of Prüm was dealt with in the symposium by different aspects.

Q317 ***Chairman:*** Indeed, yes, but I think your views on the data protection implications would be of definite interest to us.
Dr von Pommer Esche: At the start there were general statements by the Austrian Minister of the Interior and then the Netherlands Minister of Justice and the German State Secretary of the Federal Ministry of the Interior and then the experts.
Chairman: Dr von Pommer Esche, you have answered our questions extremely helpfully, it has been very useful.

Q318 ***Earl of Listowel:*** I am sorry to interrupt you, my Lord Chairman, but might I ask our witness if he has knowledge about the Schengen Evaluation Teams. If so, perhaps he could say something about the degree to which they co-operate, particularly those teams that go in to monitor after the first assessment for acceptance, whether there is sufficient co-operation between the teams and, I think it is, the national ombudsmen. I heard some concern that there is not perhaps enough co-operation on those assessments.
Dr von Pommer Esche: I have never been part of such a team. Germany was visited by such a team in the late 1990s. We also had a visit from the team at our office. A team has also visited the *Bundeskriminalamt* and they have made inspections on the borders. I do not know very much about the working methods of these teams. If new countries accede to the Schengen Treaty via the EU, then the Schengen JSA gives an opinion and in that capacity and in that context we get knowledge of the reports from these teams but personally I am not involved.

Q319 ***Chairman:*** Doctor, I wonder if I could ask rather a personal question. We all understand, and I think perhaps regret, the reasons why the British Government does not take part in immigration exchange. Can I ask you, does your agency have bilateral contact with your British opposite numbers outside the envelope of Schengen? In other words, do you have a direct bilateral exchange with your British opposite numbers?
Dr von Pommer Esche: We have a good relationship with David Smith but I would not say it is a special relationship. It is a good relationship. I would not say we have special topics to deal with jointly with our British colleagues.

Q320 ***Chairman:*** That is a very fair answer. When you see the transcript of this meeting if there is anything you think it would be useful for us to have in addition, please feel absolutely free to communicate it to us. May I, on behalf of all my Committee, thank you very much indeed. It would be impolite of me to congratulate you on your English, which is flawless. Thank you very much for coming to speak to us and for answering our questions so helpfully.
Dr von Pommer Esche: Thank you. It was a pleasure. I would also say that Mr Schaar apologises. He could not come today because this week we have a hard week because the anti-terrorism legislation in Germany is being dealt with in the Committee for Internal Affairs in the *Deutsche Bundestag* on Wednesday which will be a hard challenge for Mr Schaar.
Chairman: Would you please send him our good wishes. Thank you.

27 November 2006

Examination of Witness

Witness: MR GERRIT HUYBREGHTS, Directorate-General, Justice and Home Affairs, Council Secretariat, examined.

Q321 ***Chairman:*** Mr Huybreghts, thank you very much indeed for coming to give evidence to us. For the record, this meeting is, of course, on the record, although at any point if you want to go off the record, you are very welcome.
Mr Huybreghts: Okay.

Q322 ***Chairman:*** A transcript of the meeting is being taken and in due course you will be sent the transcript for you to confirm that it correctly reflects what you have said. This is scrutiny by a House of Lords sub-committee into Schengen II, or SIS Mark II, however we care to refer to it. I think we have given you notice of our questions in advance. Could I start, please, with the first question which is whether the Council prepares annual statistics on the functioning of the SIS and, if not, do you not think that they should?
Mr Huybreghts: Okay. Can I make an opening statement first?

Q323 ***Chairman:*** Please do.
Mr Huybreghts: I have to inform you of the limits within which I work.

Q324 ***Chairman:*** Of course.
Mr Huybreghts: I work for the Council Secretariat, so I do not represent the Council and I do not represent the Council Secretariat. I asked permission to come here and I got permission but I speak on my own behalf. As Council Secretariat we support the presidency and assist the working groups within the Council, but we should have some discretion as to the positions of delegations from different countries. I am also aware of a number of issues that I should not talk about so I will indicate that there is nothing further I can say.

Q325 ***Chairman:*** Of course.
Mr Huybreghts: As Council Secretariat we have to be strictly neutral politically, so in a number of cases I will not be able to comment on opinions because we simply do not do that.

Q326 ***Chairman:*** No.
Mr Huybreghts: If I could start by introducing myself.

Q327 ***Chairman:*** Please do.
Mr Huybreghts: My name is Gerrit Huybreghts, I am Belgian. I have been working on the Council Secretariat since 1990. I entered as an IT specialist and later joined the so-called political side and started to work as a meetings secretary. I worked on the IT side between roughly 1990 and 1999. In 1999 the Schengen Secretariat was integrated into the Council Secretariat and at that moment I started to work for SIS. As such, I have been working as a meetings secretary for the SIS Technology Working Groups. I have worked on SIRENE matters and did a follow-up of the SIS II project and took part in Schengen evaluation missions. That gives a general description of what I do. You refer to me as a Council expert on statistics, which is a little bit of an exaggeration. Statistics is one of the things that happened but I am not an expert on statistics. The first question, whether I would consider that the Council should do that, is a political question so I cannot go into that. Until 1999 when the Schengen co-operation was within the Schengen Secretariat there was an annual report made by C.CIS, which is the central body located in Strasbourg. When all of this was integrated into the European Union, apparently at that moment they stopped making yearly reports, so there were no more yearly statistics. It was only in 2005, because of remarks that were made in the European Parliament about secrecy in relation to the number of data in SIS and because of questions from the academic world, that the presidency took the initiative to publish yearly statistics but without giving details about the different Member States. I have copies of the last two for the Committee if you want these.

Q328 ***Chairman:*** Thank you very much. That is the available documentation that you referred to?
Mr Huybreghts: Yes. I did not know how many of you there were but I have made a number of copies.

Q329 ***Chairman:*** Thank you very much.
Mr Huybreghts: I have copies of three documents. One is a document on the SIS database statistics as of 1 January 2005 and the next one is as of 1 January 2006. Then I have a table of hits that were recorded. This table of hits is the 2006 version but if you have a look at it you will see that it gives an overview from 1997 to 2005.

Q330 ***Chairman:*** Thank you very much. I do not want to draw you into answering political questions, I quite understand your reservation on that, but can you explain why are statistics regarded as controversial? What problems does that raise?
Mr Huybreghts: As I explained, at one point these were made and sent to the different governments but as soon as it stopped the habit was lost and when it was tried to start it up again everyone—

Q331 ***Chairman:*** Were they stopped because of a controversy?
Mr Huybreghts: No, just because at the point of the integration of the Schengen Secretariat within the European Union there was no demand made to publish those yearly overviews any more, so it just stopped.

Q332 ***Chairman:*** It just fell away.
Mr Huybreghts: Yes. When you try to start again everybody wants to know why you want to publish statistics. This was more or less what happened. There is a sensitivity on the sides of the different delegations to give national data. As you will see, from the statistics on hits that document was made public without further ado.

Q333 ***Lord Avebury:*** Is any statistical information available at Council level other than that which is contained in the papers that are now distributed, which unfortunately I have not yet been able to see? Are there any additional statistics collected by some or all Member States which are not necessarily presented to the Council, for example regarding the practical use of SIS I made by national authorities?
Mr Huybreghts: Other statistical material except this one? As I explained, the yearly statistics exist with a division between the different Member States and they exist in somewhat more detail than is given there. Apart from that, not a lot of statistics are made about the SIS and available at Council level. I am sure that at the national level there are more statistics but those that I have seen differ very much from country to country. The only instance when we come across them is during a Schengen evaluation mission when additional data is asked for and then we find out that they exist, but they are only used for the year before the evaluation is made. There is no large scale exercise in statistics for SIS I.

Q334 ***Chairman:*** Does this information include available material from the United Kingdom and Ireland?
Mr Huybreghts: There is no information about—

Q335 ***Chairman:*** None?
Mr Huybreghts: No. Since they do not participate they are not yet operational in the SIS.

Q336 ***Chairman:*** In the full SIS, that is right.
Mr Huybreghts: Not in the full SIS and not in the partial SIS.

Q337 ***Baroness Bonham-Carter of Yarnbury:*** Can the statistics on the use of SIS II be linked to statistics available at national or EU level relating to extradition requests, visa refusals, refusals of entry at the border, and refusals to renew or grant residence permits?
Mr Huybreghts: No. It is simple. You asked that question before. In the Schengen Information System we have alerts for unwanted aliens, so-called Article 96 data. The finalisation of that is refusal of entry at the border. I have provided you with the statistics on hits but these statistics are of very poor quality as regards Article 96 data. Maybe I should explain a little bit how the statistics are made. A hit means when there is a control some person or object in the SIS is found and at that point the country where it is found sends a so-called "G-form" to the country that requested the person or object to be found. The hit statistics are based on counting the G-forms but there is no obligation to send a G-form for an Article 96 alert. The reason for that is if you have, for example, a missing minor then obviously you want to repatriate the minor and in order to do that you need to get information about the parents or the police unit that has been investigating the case of the missing minor, so the two countries have to get in contact. For Article 96, unwanted aliens, that is not done because what you have to do is refusal of entry, you do not have to contact the country in question. That is a rule that is put into the so-called SIRENE manual, a manual that describes the procedures, and there it explicitly says that there is no need to send a hit form in the case of Article 96. In the most recent version of the SIRENE manual that was published on 16 November this year there is now a new rule that says statistics will have to be provided, so the quality of statistics for refusals of entry that are based on the SIS will increase.

Q338 ***Earl of Caithness:*** In this rather frightening secrecy that surrounds this system, do you have information that is not published on such things as the use of the SIRENE system and actions taken following a hit? What I am trying to get at is how much more information do you know and have got records of that is not being released?
Mr Huybreghts: None that are systematic. As I explained, when we do Schengen evaluation we go to visit a country and ask a number of questions and at that moment you can be confronted with statistics but it is the statistics used at that moment that you get. There is no systematic collection at Council level of statistics on the national side.

Q339 ***Earl of Caithness:*** Is that because there is no requirement on the Member State to furnish you with that or is that just because there is no system within the Council to absorb them?
Mr Huybreghts: I would say both. There is a point which might help the Committee to understand this. In the present SIS you have a central system and national copies. The only task of the central system

is to make sure that the national copies are identical because it is the national databases that are really the active parts of the system. Every request to look for a person and every control that is made is made on the national systems. If statistics are made they are national because on the central side it is not possible to see if, for example, there are 100 people passing at a certain point who are controlled, that is purely a national matter. The way different countries do that is their own responsibility. There is no information available at Council level but there are no requirements because it is a national responsibility and there is no system at the Council level to collect and absorb it.

Q340 ***Lord Dubs:*** Is information available about the impact on SIS of the application of the European Arrest Warrant, and of the amendments to the current SIS rules adopted in 2004 and 2005, and applied in 2005 and 2006?
Mr Huybreghts: The application of the European Arrest Warrant, as far as I know, has had no dramatic impact on the SIS. The only impact it has had is on the so-called "flagging". I do not know whether you are familiar with the term.

Q341 ***Lord Dubs:*** Yes.
Mr Huybreghts: Flagging means when one country asks to arrest a certain person, for the reasons of that country the country can say that it does not want to act on that. That is called putting a "flag" up. One of the main reasons for flagging was the fact that countries did not extradite their own nationals. In the European Arrest Warrant it was agreed that should happen, countries should extradite their own nationals. The number of flags that are put is likely to diminish, and the information I have is that they are diminishing. That is the only impact on the SIS of the European Arrest Warrant that I know on of the statistical side. On the other changes that were adopted in 2004 and 2005, what has happened is the length of conservation periods for certain alerts have been extended and because they have been extended you can see the numbers of data in the system to go up. That is not because more data are collected but because they are kept for a longer period.

Q342 ***Baroness Henig:*** I think there may be a political element to my question, in which case if that is a problem please say so. Would it be possible to collect further statistical information, in particular upon the impact of the Schengen Information System in Member States and the operation of the SIRENE system? What difficulties stand in the way of the collection of further information?
Mr Huybreghts: One of the problems is what the definition of "impact" is. What difficulties stand in the way of the collection of further information? Basically, as I explained, it is a system which for the large part, for the operational part, is oriented for the countries themselves, so this is purely a national matter and, therefore, at the central level you do not see that information. The impact that the SIS has had on the way countries organise themselves or organise their legal and justice systems is something I do not have any information about. I have never heard this being discussed.

Q343 ***Baroness Henig:*** So the problems are really technical in a way in aligning different Member States' systems to make some sense to have the things collected centrally.
Mr Huybreghts: It is not so much aligning rather it is the fact that the whole organisation surrounding the police and justice is very much a national matter.

Q344 ***Baroness Henig:*** What I meant by alignment was that they are operating in different ways.
Mr Huybreghts: Yes.

Q345 ***Earl of Listowel:*** Does the statistical information which is available enable us to draw any conclusions about the efficiency and operational effectiveness of the SIS?
Mr Huybreghts: The problem about questions on efficiency and operational effectiveness is that there is no exact way to measure them. You would need to have a standard. If there were two competing systems it would be possible to say "this one is the more efficient". At this moment my impression is that the statistical information does not allow us to draw any conclusions about that.

Q346 ***Chairman:*** Is it fair to ask you how SIS and SIS II compare in terms of efficiency?
Mr Huybreghts: Since SIS II is not working yet it is very difficult to say that.

Q347 ***Chairman:*** Sorry, I meant SIS II as projected.
Mr Huybreghts: Even so, it is only when it is working that we will see whether it has worked. In large part it depends on the use that people make of the information that is provided.

Q348 ***Chairman:*** Of course.
Mr Huybreghts: In the SIS II there will be much more information stored, certainly on objects. The idea is that, for example, industrial equipment will be in there and data about credit cards. That could lead to a greater impact on crime fighting but that is still to be projected. The only thing that I hear about statistics concerns the so-called Article 99 alerts. These are alerts for specific checks and discreet observation. Discreet observation means if the police spot a car and the car is subject to an alert Article 99 for discreet observation, in that case the policeman is

supposed to go over and ask a number of questions and try to find out, for example, who the persons in there are, how many they are and what their apparent business is and to report it back. In almost every evaluation that we make of that police forces should make more use of that.

Q349 ***Lord Teverson:*** What we are trying to explore is the statistics that have come out of SIS I or the existing system. How do you see those as relevant? What do they tell us about how this new system should be developed, if at all? Has that been taken into consideration in practice?
Mr Huybreghts: The present statistical material has been taken into account for the dimensioning of the system because it gives an indication of how much data there will be in SIS II, but of course for industrial equipment and credit cards, et cetera, where there is no presence yet in the SIS it is guessing.

Q350 ***Lord Teverson:*** Could I ask about that to get some idea of size. At the moment it goes up to 18 Member States and it is currently functioning on, I suppose, 13—
Mr Huybreghts: Thirteen Member States, yes.

Q351 ***Lord Teverson:*** I do not know how you measure the size of the present system but how many times larger is it expected to be, say, once the new accession states have been included? Have you got some sort of measure of that?
Mr Huybreghts: Unfortunately, no.

Q352 ***Lord Teverson:*** How many floppy disks would it take to fill up?
Mr Huybreghts: I cannot answer that, sorry. It is not that this is in any way confidential but I just do not have the figures on that.

Q353 ***Lord Teverson:*** I apologise, I interrupted your answer.
Mr Huybreghts: I have forgotten what I was saying.

Q354 ***Lord Teverson:*** That is my mistake, I apologise for that. We were talking about what had been learned from the production of statistics this time round that had been taken into consideration in the development of the new system.
Mr Huybreghts: It helps in dimensioning the system. The operational Member States were asked to provide statistics on the number of queries they made. That was in order to dimension the network that would be used. These are the only elements that were used.

Q355 ***Chairman:*** I heard you say that we wrongly described you as an expert on statistics but, if I may say so, you are showing yourself extremely expert in your replies.
Mr Huybreghts: Thank you.

Q356 ***Chairman:*** How far are you involved in developing SIS II? Is your very obvious knowledge and experience in the collection of statistical information for SIS being used? Are you part of the development of SIS II?
Mr Huybreghts: No, I am not. The development of SIS II has been given to the Commission. The Commission has taken note of the information that is available and has asked for further information from Member States. If I am not mistaken, at this moment they are trying to get an idea from the new Member States of the number of data, how many data they think they will introduce. When I spoke earlier about the fact that the number of queries has been collected, that is also something the Commission has done. On the side of the Council Secretariat I am trying to follow up as much as possible. If there are questions from the Commission side about things I know then I will provide them.
Chairman: We will be seeing the Commission tomorrow so we will bear that in mind. Thank you very much.

Q357 ***Lord Avebury:*** In reply to Lord Teverson you mentioned two examples of further information which will be contained in SIS II that is not in SIS I. Will these additional features of SIS II require changes in the statistical information which is collected? Do you foresee any problems in collecting information for the regular reports which are required by the legislation on SIS II? Could I ask you in particular what information will be collected on the relative frequency of one-to-one and one-to-many searches based on biometric data? Will there be any difficulty in collecting information for the regular reports on the operation of SIS II which are required by the legislation?
Mr Huybreghts: On the biometric data I am not aware of any specific collection of information or statistics. I believe you have had sessions before on the biometrics where you were informed that the one-to-many searches would only be installed after a report by the Commission.

Q358 ***Lord Avebury:*** Yes.
Mr Huybreghts: So everyone is waiting until that report for action. Whether it will be difficult to collect statistical information, it always is. It is difficult with 15 Member States participating and once it is 25 or 27 it will be more difficult to get discipline with all the states in order to get information. That said, I suspect that in the new system there will be more automatic

ways of collecting information. One difference is that now you can extend the period of an alert. For the SIS II it will be required to make statistics available about that which are not available at this moment. In the new legislation there will be a request to have statistics on the number of queries that are made, the number of consultations, which is something that is not collected today.

Q359 ***Baroness Bonham-Carter of Yarnbury:*** Is it planned to collect information in relation to the use of SIS II for asylum applications as far as you are aware?
Mr Huybreghts: No, not specifically. In that respect I have to tell you that the Council publishes a yearly overview of all authorities that have direct access to the SIS and at this moment only Austria gives the asylum authorities access to the SIS, which in the present system means that if there is a statistic anywhere about asylum applications in the SIS it would be in Austria. It is purely a national statistic.

Q360 ***Earl of Caithness:*** Do you know if any of the data protection authorities make use of your statistics? If they do not, is there is anything in your statistics that might help the data protection authorities?
Mr Huybreghts: Well, data protection authorities often have access to statistical information. I know that the Joint Supervisory Authority at one time published a very detailed statistical analysis of the Schengen Information System, the kind of data that I would not be allowed to give you! Sometimes on the internet statistics of the same kind circulate that I would not be allowed to give to anyone. On the actual use, the Joint Supervisory Authority at one point made a report about the application of Article 96 alerts, the alert for unwanted aliens, and they based the question that they wanted to treat partly on available statistics. These statistics showed that the numbers of alerts differed widely between the different Member States, which indicated that the criteria for issuing an alert pursuant to Article 96 differed from Member State to Member State. This led to a request for more harmonisation, a request that was also voiced by the European Parliament in their discussions on the SIS II. This is one way in which the Joint Supervisory Authority makes use of the statistical information. The other point, perhaps one for the future, is since 2005 we have had regulation on the access of car registration authorities to the SIS. The Council has to submit a yearly report to the European Parliament on the way these authorities make use of the SIS. It has also said that the Council should contact the Joint Supervisory Authority and the report should contain how the data protection rules have been applied. There will be an interplay between the Council and the Joint Supervisory Authority on the way the data protection is applied under this regulation.

Q361 ***Chairman:*** When you say there is certain information that you are unable to give us, or perhaps not allowed to give us, is this because of the sensitivities of individual Member States?
Mr Huybreghts: Yes.

Q362 ***Chairman:*** And sensitivity about comparisons between Member States?
Mr Huybreghts: That is my general impression, yes. Sometimes I get the reaction that delegations consider if another Member State has more alerts for a certain type of object they could be asked questions why they do not work more to get the same. It is that type of comparison that everyone wants to avoid.
Chairman: Or "I have more criminals than you have"!

Q363 ***Earl of Caithness:*** Going back to the relative halcyon days of the Schengen office by itself before it got absorbed into the Commission, can you provide us with a copy of the information that the Schengen office released annually, its annual report? Is that possible, so that we can see what it did do?
Mr Huybreghts: I would have to look for that because it was before my time. I do not know where I could find it. I can try to find it.

Q364 ***Earl of Caithness:*** Could you try because that would be very helpful to us.
Mr Huybreghts: Okay, I will have a look.

Q365 ***Chairman:*** Perhaps I should say on that point that if, when you come to look at the transcript of this meeting, you think there is any other supplementary information that it would be helpful for us to have, we would be very grateful to have it.
Mr Huybreghts: Okay.

Q366 ***Lord Dubs:*** What additional information might be collected if European information systems became interoperable? It is a bit speculative as a question, I appreciate that.
Mr Huybreghts: It is one that has drawn the attention of a lot of people, the interoperability of information systems. Are you specifically referring to statistical information or information in general?

Q367 ***Lord Dubs:*** Probably statistical. No, I would not want to say only statistical.
Mr Huybreghts: On statistics, you have seen the amount of statistical information that is available in the Schengen Information System, so I do not think that interoperability will lead to more helpful information. Interoperability in itself is an issue that has been hotly debated. One point is that in the

debates about interoperability between information systems, certainly in justice and home affairs, if you look at the documents there are different types of interoperability described and each one has its own merits or not. There is one interoperability issue which is simply between communication systems that is purely technical; is one system able to communicate with another? That does not give any information about the content, so that is not useful in this respect. One other method of interoperability is the fact that you give common access or simultaneous access to two different databases. That could lead to more information but the way the SIS is organised is as a transactional system in the sense you have one question about one person, for example, and you send that to the database. If you have access to two databases at the same time you could see whether that same person is in two databases. That could be information but that type of supplementary information is coincidental, it just happens. It is not allowed to do searches in the SIS where you say, "I want to find all people from Arab countries between 20 and 40", for example, and compare that with what is available in another database. Because of the way that the Schengen Information System works, and the justice and home affairs databases in general, this type of interoperability will not help very much. In general, I think interoperability will not lead to very much more information. That said, there may be a request at one point but I find that most of the operational services are usually not really defending interoperability between different information systems, which probably means that it looks like a good idea but on the practical side nobody really sees what the advantage is. That is the impression I have got. That is rather a personal opinion, but anyway.

Q368 ***Baroness Henig:*** To what extent are the current SIS statistics, and future SIS II statistics, relevant to the Commission's proposals for legislation on immigration and asylum statistics, and for an action plan on EU crime statistics?
Mr Huybreghts: I am afraid I do not think there is any relevance.

Q369 ***Baroness Henig:*** So the answer is none?
Mr Huybreghts: I have seen a document from the Commission on improvement of crime statistics and it mentioned the fact that one of the problems was that crime statistics were organised very differently in the different countries, which is more or less the same thing I am saying about SIS statistics, so there is a relevance in that sense but it is rather negative.

Q370 ***Baroness Henig:*** So by the time you have made allowances for all the different ways in which the statistics are collected and the categories and so forth, there is not much left is what you are saying, there is not enough common information.
Mr Huybreghts: Right.

Q371 ***Baroness Henig:*** Is there any way round that?
Mr Huybreghts: No. One of the specificities of the SIS is you get a selection of persons and objects that are wanted. For example, on cars in a number of countries there is a limit to the number of cars you put in which in some Member States is a financial level, if a car is worth less than X euros there is not much sense if it is found on the other side of Europe in repatriating it because the cost involved will be greater than the cost of the car. The same goes for people who are wanted for arrest. A decision has to be made as to whether or not that person should be subject to international arrest, which means you have a selection. In my view you cannot derive general conclusions about crime statistics in the different countries based on the information in the SIS because there is so much selection that has to be done by the national authorities.

Q372 ***Earl of Listowel:*** Perhaps it follows from what you have said that the following question may not be so helpful, but could you say whether the current SIS statistics, and future SIS II statistics, including further statistical information on the SIS which might be collected, would be of use in the development and evaluation of EU justice and home affairs legislation?
Mr Huybreghts: First of all, this is a little bit outside my sphere of knowledge. As a general guess I do not think it would be very helpful.

Q373 ***Chairman:*** Rather similar to the answer to the previous question.
Mr Huybreghts: Yes.

Q374 ***Lord Teverson:*** On the question of Article 96 alerts, this question was really whether analysis is available by Member States of the different reasons why those alerts have been made, say between immigration or criminal acts, different reasons for Article 96 alerts.
Mr Huybreghts: I am not aware of any studies about that.

Q375 ***Lord Teverson:*** Is it possible for the system to differentiate between the different reasons?
Mr Huybreghts: No, I do not think so.

Q376 ***Lord Teverson:*** Could I ask one other question. Is there any estimate of the amount of the proportion of information in the Schengen I Information System that is incorrect, or the error entry rate?

Mr Huybreghts: That is a difficult question. I know when the Joint Supervisory Authority looked at the Article 96 data that at one point there were remarks about the number of alerts that they have studied more in-depth and from that I believe they derived an error rate. I would say that is a question you should ask the Joint Supervisory Authority because they would have more of this data than I have seen. The other factor is about the quality of data and that has been a thing that has come up during the years. I am not too sure how that is working now but CSIS, together with the Member States, at one point worked out a list of quality criteria and on that started quality monitoring. I believe it is weekly monitoring that is sent to the Member State where they can see whether there is information that is probably not correct. I know on certain data we found at a certain moment there were entries saying "unknown" but in 12 different languages which made everybody jump up and say, "This has to go". This type of thing happens. For those things where there is knowledge of what goes wrong, CSIS has tried to start up monitoring and the results are sent to the different Member States and it is up to them to take action.

Q377 ***Lord Teverson:*** Do you have any feeling?
Mr Huybreghts: No, because it is sent to the different Member States in order for them to take action. What happens is that every three months there is a comparison of the national databases with the central database. It is the task of C.CIS to make sure that the data are the same everywhere, so every three months a comparison is made and each Member State gets a list of where there are problems and these then have to be corrected.

Q378 ***Lord Teverson:*** That has to be reconciled?
Mr Huybreghts: Yes.

Q379 ***Lord Teverson:*** Every difference has to be reconciled?
Mr Huybreghts: Yes.
Chairman: Mr Huybreghts, thank you. I hope we have not drawn you too far into the political arena, we have tried to avoid that. I am very grateful to you for your very frank and full and helpful replies to our questions. Thank you.

TUESDAY 28 NOVEMBER 2006

Present	Avebury, L	Henig, B
	Bonham-Carter of Yarnbury, B	Listowel, E
	Caithness, E	Teverson, L
	Dubs, L	Wright of Richmond, L (Chairman)

Memorandum by Jonathan Faull, Director General, Justice, Freedom and Security European Commission

1. The SIS is a vital tool for the smooth running of an area of freedom, security and justice. It contributes to the implementation of the provisions on the free movement of persons (Title IV of the EC Treaty) and to police and judicial cooperation in criminal matters (Title VI of the EU Treaty).

The Decision Making Process Which has Led to the Development of the SIS II, Particularly the Adequacy of Public Consultations and Lack of Impact Assessment

2. The Decision and Regulation on the development of a second generation of the SIS (SIS II) was taken by the Council in December 2001.[1] The Council[2] had in mind the enlargement of the Schengen Area to the Member States that were going to join the EU in May 2004 and which required a new SIS. In addition, the SIS II had also to benefit from the latest developments in the field of information technology. These legal acts also provided for the inclusion in the budget of the EU of the necessary appropriations for the development of such a system. It should be noted that the current SIS is funded on an intergovernmental basis.

3. This decision of the Council to develop a new SIS entrusting to the Commission the technical implementation was taken without prejudice to future legislation that would lay down in detail the operation and use of the system.[3] This was precisely the objective of the three proposals submitted by the Commission in May 2005 that shall govern the SIS II and that need to be adopted before the new SIS can start operations. Two out of these three proposals follow the co-decision procedure, which allows the European Parliament to play its role fully as legislator on this sensitive dossier.

4. The current SIS has proved its efficiency and added value for maintaining a high level of security in an area without internal border controls. The SIS II should offer at least the same services as the current SIS and shall include the possibility, if confirmed by the legislator, of providing some new services or functions. The underlying rationale and nature of the system will remain the same as the current SIS. An impact assessment and public consultation were, therefore, not necessary. However, when drafting its proposals the Commission took into account the comments made on the current SIS by national experts, the Schengen Joint Supervisory Authority and other organisations, and it formally consulted several bodies active in the field of data protection on the proposal adopted: the European Data Protection Supervisor, the Schengen Joint Supervisory Authority and the Article 29 Working Party.

5. The Commission started the technical implementation of the SIS II before the legal package was presented in order to keep the tight deadline for having the system in place, which will allow, if the other legal criteria are met, the enlargement of the area without internal border controls to the Member States that joined the EU on May 2004. However, the final decision as regards the operations, use and functionalities of the system, personal data protection and access rights lies exclusively with the EU legislator. The Commission is reviewing regularly the technical implementation of the SIS II to ensure that it is perfectly in line with the legal acts as being negotiated and to be adopted by Council and Parliament.

Operational Management of the SIS II

6. The Commission proposed that it should initially be responsible itself for the management of the SIS II because this would ensure continuity between the system's development and operational phases. However, it has become evident throughout the inter-institutional negotiations that it is not an option for the long-term that is acceptable to Member States or the European Parliament. In the light of the latest results of the

[1] Council Decision 2001/886/JHA and Council Regulation 2424/2001 of 6 December 2001.
[2] cf recitals 2, 3 and 4 of both legal acts.
[3] cf recital 7 of the aforementioned legal acts.

negotiations, it seems that the management will be divided into two phases: an interim phase and a long-term phase. During the interim period the responsibility for the management will lie with the Commission, which will have the possibility to delegate operational management tasks to public authorities of Member States. The long-term management of the SIS II will be most likely given to a European Agency, although the Commission will carry out an impact assessment study to identify the best option.

7. Whatever solution is chosen for the management, it will have to guarantee a sufficient level of accountability and transparency. The Council and the European Parliament should have a say on the rules of functioning of the management body and it will function within the EU inter-institutional system of checks and balances. The management body will have to present regular reports on the technical functioning of the SIS II and the Commission shall produce and transmit to the Council and the European Parliament on a regular basis an overall evaluation of the central SIS II and the exchange of supplementary information between Member States. The evaluation will include examination of results against objectives, assessment of the validity of the underlying rationale, the application of SIS II legal instruments and any implications for future operations.

The Implications of Including Biometric Data

8. The possibility of processing biometric data (fingerprints and photos) was requested by the Council in its conclusions on the SIS II in 2003 and 2004. The intention is initially to store and retrieve this type of data for confirming identifications performed on the basis of an alphanumeric search. The photos and fingerprints would allow the police officer or border guard to verify whether the person being checked is the same as the one intended by the alert in the SIS. At a later stage fingerprints could be used for searching the database alone or in combination with the alphanumeric data.

9. Identification by using biometric data has not only proven its reliability in national police systems but also in EU large-scale IT systems such as EURODAC for the identification of asylum seekers and it is also an intended functionality for the Visa Information System (VIS). This use of biometric data should not imply any change in the nature of the system since the legal framework clearly limits the use of the system. In practice this new functionality would mean, for instance, that a border guard when checking a person against alerts for refusal of entry at the external border will not only use the name, date of birth or other alphanumeric data, but can also collect the biometric data from the person or from the passport in order to perform the identification.

10. In general the use of biometric data should increase the quality of the database and of the searches leading to more reliable identification. This should also improve the situation of people suffering the consequences of misidentification performed by the current SIS based on simple alphanumeric searches.

The Provisions Allowing the Interlinking of Alerts

11. Links between alerts should only be introduced when there is a clear and well-defined relationship between them. They will not affect the specific action to be taken on the basis of each of the linked alerts or their conservation periods. Moreover, they will not affect access rights to the alerts since a link will be only seen by the authorities having access to both of the linked alerts.

12. As this will be a new functionality it is difficult to anticipate the use that Member States will make of it. The intention is to draw the attention of the officer who has spotted a person or an object in the SIS to other possible alerts in the system that would allow him or her to take another action.

The Criteria for Listing Persons to be Refused Entry

13. The Commission proposed to harmonise further the conditions or criteria for entering alerts in the SIS II for the purpose of refusing entry given the diverging practices of the Member States. This has been confirmed not only in reports of the Schengen Joint Supervisory Authority or independent human rights reports, but also in meetings of national experts. However, the two main criteria proposed for issuing such an alert—threat to public policy or security and illegal immigration—remain the same as in the current Schengen Convention.

14. The Commission has added to these two basic criteria a new one targeted at third country nationals who are subject to restrictive measures intended to prevent entry or transit through the territory of the Member States in accordance with Article 15 of the EU Treaty.

15. Council and Parliament seem to agree on the aim to achieve a higher level of harmonisation regarding the criteria for issuing these alerts although this level will remain lower than the Commission proposed initially. The legislators seem also to agree that the Commission shall review the application of the provisions concerning the issuing of these alerts in view of achieving a higher level of harmonisation in the future.

The Appropriateness of Including Third-country National Family Members of EU Citizens in the SIS II

16. Schengen cooperation must be fully compatible with EU/EC law. The European Court of Justice has stressed this fundamental point in its recent judgment of 31 January 2006 (Case C-503/03, *Commission v Spain*). The ECJ ruled that Spain breached Community law by refusing entry to two Algerian nationals, spouses of EU citizens, solely on the grounds that an alert for refusing entry has been issued for them in the SIS by another MS. The Court stated that closer cooperation in the Schengen field must be conducted within the legal and institutional framework of the European Union and with respect for the Treaties. Since the concept of public policy within the meaning of the Directive 64/221/EEC does not correspond to that in the Schengen Convention, a Member State which consults the SIS must be able to establish, before refusing entry to the person concerned, that his or her presence in the Schengen area constitutes a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society in accordance with the aforementioned directive. The existence of an alert in itself is not sufficient to establish this.

17. The Commission proposed initially to exclude family members of EU citizens from the scope of the Regulation. However, Member States, fearing that it could undermine security in the area without internal borders, prefer to have the possibility to introduce alerts on third-country nationals even if they are family members of EU citizens. In the event that this option will be accepted by the Council and the European Parliament, it has to be accompanied by appropriate safeguards guaranteeing that EU legislation on free movement is respected.

The Clarity of the Rules Governing Collection of and Access to Data, Including the Desirability of Granting Access to Immigration Data to Police and Asylum Authorities

18. The Commission intended to improve the current rules regarding the collection of data, in particular the conditions for issuing the alerts in the SIS. The general conditions that are part of the basic legal framework will be completed with implementing measures containing technical rules for entering and searching the data in the SIS II. These rules should improve the overall quality of the database and increase transparency regarding the functioning of the system.

19. Access rights to data must be provided following the purpose of the alert. It is clear that the access to data for refusal of entry could only be provided in the context of the Regulation which regulates the use of the SIS in the control of external borders, visa issuing or more in general immigration control or policing.

20. The SIS II legal acts do not appoint the authorities with right of access; they provide for access rights to the SIS II on the basis of the tasks to be carried out. For example, if the police in a Member State has responsibilities for border checks or immigration control then it shall have access to the alerts for the purpose of refusal of entry. However, if the access to these alerts is performed for the purposes of the prevention, detection and investigation of criminal offences such a use must be regulated in the third pillar act—Decision—with a bridging clause in the Regulation that will make the immigration data available for purely police purposes.

21. In its proposal the Commission has also provided for access for asylum authorities to alerts for refusal of entry for two different purposes. The first purpose is the application of the Dublin Regulation[4] which reflects the practice of some Member States where these authorities have access (direct or indirect) to these alerts. The objective is to identify whether another Member States is responsible for an asylum application based on the responsibility for the illegal entry or stay of the asylum applicant in a Member State. The second purpose relates to the application of the Directives on minimum standards on procedures in Member States for granting and withdrawing refugees status and on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection.[5] The intention is to ensure via the SIS an efficient exchange of information between Member States for

[4] Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national *Official Journal* L 050, 25/02/2003.

[5] Directive 2005/85/EC and Directive 2004/83/EC.

performing security checks on asylum applicants and to facilitate the implementation of provisions contained in the aforementioned Directives concerning exclusion from refugee status or the possibility of launching an accelerated or prioritised examination procedure.

22. In any case it must be underlined that in the context of asylum the fact that the person is found in the SIS can never immediately or automatically lead to a refusal of refugee status or to a transfer of the asylum seeker to another Member State in accordance with the Dublin mechanism. The alerts in the SIS only constitute INDICATIVE information that will allow the competent authority to make a more informed decision and, therefore, to apply Community rules more effectively.

The Adequacy of Data Protection Rules, in Particular as Regards Data Which Might be Transferred to Third Countries

23. With regard to the first-pillar Regulation, EC data protection rules will apply, in particular Directive 95/46/EC and Regulation No 45/2001. With regard to the third pillar Decision, the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data will apply. It will be replaced by the Framework Decision on data protection in the third pillar after the adoption of this proposal.

24. In its proposal the Commission excluded the transfer of data to third parties with some limited exceptions. The SIS II draft Decision provided for transfer of data to third countries or organisations in the framework of an EU agreement with third parties guaranteeing an adequate level of protection of the transferred personal data and with the consent of the Member State that entered the data.

25. From the ongoing discussions it has become clear that the scope of the exception from the general rule of not transferring the data will be even more limited. The only exception would be exchange of data on passports with third countries via Interpol with appropriate data protection safeguards.

The Implications of the Plans on Interoperability of EU Databases

26. From a technical perspective "Interoperability" is the ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge. This is disconnected from the question of whether the data exchange is legally or politically possible or required.

27. The Commission's Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs presents different scenarios on how the existing large-scale IT systems could, in addition to their existing roles, more effectively underpin the policies linked to the free movement of persons and contribute to the fight against terrorism and organised crime. The aim of the Communication was to provide a global picture and start a general debate at Council and Parliament on possible developments in this field. Following this debate and after a careful assessment, in particular from a fundamental rights perspective, more concrete steps could be taken in order to promote interoperability and ensure the flawless exchange of data between the existing or even future IT systems in the field. These concrete steps would also include the relevant impact assessment and legislative proposals amending the legal framework of the existing IT systems.

The UK Position on the SIS, Particularly the Need for Access by the UK to Immigration Data

28. The SIS is essential for maintaining a high level of security in an area without border controls. Following the UK's request, the Council decided on the participation of the UK in the Schengen Acquis limited to the aspects linked to the police and judicial cooperation in the criminal field. This has excluded the UK from participating in the exchange of information performed via the SIS aiming at the control of external borders or issuing of visas since it does not participate in these common Schengen policies. Therefore, the UK has no access to alerts for the purpose of refusing entry.

29. Access for the UK asylum authorities to alerts for the refusal of entry for the implementation of the aforementioned asylum directives, similar to that available to other Member States, is excluded since, as explained above, the UK is not taking part in the SIS II Regulation. An *ad hoc* solution allowing an indirect access for UK authorities could be examined once the SIS II legal acts, including the provisions on access rights and purposes, have been adopted.

28 July 2006

28 November 2006

Examination of Witnesses

Witnesses: MR JONATHAN FAULL, Director, DR FRANK PAUL, Head of Unit, and MRS MARIE-HÉLÈNE BOULANGER, Official, Directorate-General for Justice, Freedom and Security, European Commission, examined.

Q380 ***Chairman:*** Thank you very much indeed to the three of you for coming. Particular thanks for coming here to meet us rather than us going to meet you, it is very good of you. It is very nice to see you again. If I may say so, you are becoming quite a friend of this Committee.
Mr Faull: I hope you say that afterwards.

Q381 ***Chairman:*** I hope the friendship will last the session!
Mr Faull: Exactly.

Q382 ***Chairman:*** Can I say that this meeting is on the record. If at any point you want to go off the record, you are entirely welcome, and that busy pen will be put down. You will be sent a transcript in due course. Just for the record, this is a Lords sub-committee scrutiny into Schengen II. Can I also thank you for the written evidence you sent us in July, which is extremely helpful. I hope you will forgive us if some of our questions appear ignorant of the things you told us in July but it is quite helpful sometimes to have things again on the record and, indeed, to give you the opportunity to add anything you want to say. Can I start off, please, by asking do you think that the process of negotiating Schengen II legislation was transparent enough both in terms of the public and national parliaments? Do your plans to increase transparency within the European Union include any initiative to increase transparency as far as the co-decision process is concerned? Can I just add to that, that we took evidence yesterday and it sounded to us as though quite a lot of the information collected from Member States is not published. Our question is, is publication not essential to enable functioning of the SIS to be properly evaluated?
Mr Faull: Thank you, and good morning to you all. It is a pleasure to be here.

Q383 ***Chairman:*** For the record, would you just like to introduce yourself?
Mr Faull: I will introduce myself and my colleagues with pleasure. My name is Jonathan Faull, I am Director-General of Justice, Freedom and Security in the European Commission. On my left is Dr Frank Paul who is Head of Unit in my Directorate-General dealing with the large-scale computer systems including the Schengen Information System. On my right is Marie-Hélène Boulanger who works on the Schengen Information System with Frank in his unit. If I may go straight into it, the question of transparency is a very important one and it is not one wholly in our hands. The transparency of a legislative process is a matter both of the rules governing it and for the legislative institutions of the Union, essentially the Council and the Parliament of course. Therefore, the Commission is not solely responsible, not even mainly responsible I would say, for the degree of transparency that can be attained in this area. It may be important also to preface a more substantive reply with a brief comment recalling that the Schengen Information System, indeed the Schengen system more generally, were born as intergovernmental initiatives and, therefore, outside the mainstream system of making law and policy in the European Community. That has gradually been changed over the years as the system has been communitarised, as we say in our jargon, but there are still some intergovernmental aspects to it which may explain some of what may be perceived as limited transparency. The legislative proposals that the Commission made for the SIS II system are, of course, extremely important and a certain amount of urgency has been attached to their adoption because, as you will be aware, there is considerable pressure on all of the European institutions to get the Schengen Information System second generation up and running as soon as possible so that political decisions which will be needed at the end of the day to admit the new Member States to the Schengen area can be taken. People rightly want decisions to be made as quickly as possible. SIS II is an essential part of that process. That is why we all tried to secure the adoption of the set of legislative instruments in first reading and, therefore, a certain amount of pressure was put by others on us, and by us on the Council and the Parliament, to keep things moving. Discussions in the Parliament, of course, are held in public and before the voting and first reading in the Parliament on amendments to the drafts there was a public debate on 23 November at which the Vice-President of the Commission, Franco Frattini, spoke. The co-decision process between the Council and the Parliament really is a matter for them. We support the maximum transparency in that process consistent with the law and consistent with what those two institutions believe is appropriate. Therefore, we supported generally the European Council's initiative in June 2006 to improve transparency in the Council and in particular in the co-decision process, and the Joint Declaration on Practical Arrangements for Co-decision which dates back now to 1999 and is currently being revised in

order to improve transparency. There are a number of general initiatives underway and on this specific initiative we have done what we can.
Chairman: Thank you very much. Your mention of Commissioner Frattini reminds me to ask you, please, to send him my warm personal regards. I was very happy to see him in Helsinki last week.

Q384 ***Earl of Caithness:*** Director-General, you have said that it was a political decision not to publish a lot of the statistics but there seems to have been a lot more information that was available when there was the Schengen office but as soon as it came to the Commission that information was no longer made public. Was that a political decision or a bureaucratic decision?
Mr Faull: I am not aware of any policy decision to withhold information that was previously made available under the former system. May I ask my colleague, Frank Paul?
Dr Paul: Are you referring to statistics on the number of alerts, et cetera?

Q385 ***Earl of Caithness:*** Yes. From the evidence that we got yesterday there seemed to be much less information available.
Dr Paul: The answer is straightforward because the SIS I, the current system, is already operational so there are alerts and there are data. Because the SIS II is still under development there are no data because the system is not yet operational. By definition, there are no alerts whatsoever in the system which explains why there are no statistics.

Q386 ***Earl of Caithness:*** I am sorry, my question was not clear to you. The information we got yesterday was that there was more information available when SIS I was controlled by the Schengen office but when it moved into the Commission that information was no longer made public.
Dr Paul: I am not aware of what sort of information we would not disclose or what sort of information we might withhold in relation to any information that would have been made public by the SIS I. The current system is managed by the Council, it is not managed by the Commission, that has to be made very clear. We are only managing a system that is currently under development and I think we have been very transparent in everything we do. For instance, every six months we publish a report to the European Parliament and the Council on the development of the SIS II. We regularly send all the minutes of the SIS II committee, which is a comitology committee, to the Parliament as well. I think there is maximum transparency in everything we do related to the SIS II. I strongly believe that in comparison with the current system, the SIS I-plus, we have significantly increased transparency.

Q387 ***Chairman:*** Can I ask a question. In your very helpful note of 28 July you say: "The underlying rationale and nature of the system, ie SIS II, will remain the same as the current SIS, an impact assessment and public consultation were therefore not necessary". I do not know whether in the light of the passage of time you want to add anything further to that. The question, to which you have given an answer, is why did you not consider an impact assessment necessary? The second is, why did the explanatory memorandum of the proposals not explain the text of the proposals in any way?
Mr Faull: I believe that is still correct. The essential position we took was that because in most respects, and I will explain the others, the SIS II responds to the same needs and policy requirements as SIS I there was no need for an elaborate new impact assessment. Where there are new features there will be impact assessments, and I will come to that in a minute. The purpose and objectives of SIS II, we believe, are basically unchanged. The current text under negotiation between Council and Parliament says, "The purpose of SIS II is to ensure a high level of security within an area of freedom, security and justice, including the maintenance of public security and public policy, and the safeguarding of internal security and national security in the territories of Member States, and to apply the provision of Title IV of the Treaty relating to the movement of persons in their territories using information communicated by this system". That, I think, shows that the underlying rationale and nature of the system are essentially unchanged as I wrote. Nevertheless, when drafting our proposals, we took into account the comments made on SIS I by national experts, by the Schengen Joint Supervisory Authority and by other organisations as well as opinions which have been set out by the European Data Protection Joint Supervisory, the Article 29 Working Party. Where new functions of considerable importance are involved, the full use of biometric data and its use for searches, there will be a full prior assessment by the Commission before that option is made available. That has been agreed in the discussion between the Council and the European Parliament: "Before this functionality is implemented in SIS II, the Commission shall present a report on the availability and readiness of the required technology on which the European Parliament shall be consulted". Our conception of that is that there will be an assessment of the impact as well. I understand your concern that there was no commentary in the explanatory memorandum on the actual articles of the three legal proposals. We are under considerable pressure to keep these explanatory memoranda as short as possible. We believe that we did provide enough substance for people to understand and, indeed, to comment on

what was proposed. If we make excessively long texts, that leads to delay because they all have to be translated, of course.
Chairman: I applaud the aim of that statement. We will come back to biometrics later on, if we may.

Q388 ***Lord Avebury:*** I wonder if the Commission is happy with the texts which are currently under negotiation between the Council and the Parliament in the light of the considerable amendments to the initial proposals. Have you any comments to make in particular about the report from the European Parliament issued by the rapporteur on 13 October, which presumably was the subject of the debate on 23 October to which you referred in your previous answer?
Mr Faull: Is the Commission ever happy? That is an interesting question. As usual, we had a high level of ambition in the proposals we initially made but in the legislative process as it unfolds it usually turns out to be the case that more realism prevails. While we can at the end of the day be satisfied that the Community interest in which we make legislative proposals is served by the text to which the Council and Parliament agree, we may also believe that the Community interest would have been better served if a higher level of ambition had been reached. In this case we do believe that we have the requisite basis for a successful Schengen Information System to be set up. If I may take a series of points to comment on, I think we can say we are satisfied overall. Regarding alerts for refusals of entry, the conditions for issuing alerts have been tightened when dealing with cases of threats to public policy or public security. An individual assessment will have to be carried out before an alert is entered on a third country national in the SIS II, which means that collective decisions concerning several people will not be allowed. We have taken account of recent case law from the Court of Justice on the situation of family members of citizens of the European Union. Directive 2004/38 came out and account had to be taken of that. The new legal framework will allow the issuing of SIS alerts on the basis of restrictive measures taken in accordance with Article 15 of the Treaty on the European Union intended to "prevent entry into or transit through the territory of Member States, for example common positions reached to implement UN Security Council travel bans for terrorist groups". All of that is important and has been taken into account. We believe the data protection regime is satisfactory. We have applied the Community's data protection rules to the processing of SIS II data for the purposes of refusing entry or stay. We have secured central supervision in the sense that supervision of data processing done at the central site will be under the responsibility of the European Data Protection Supervisor in co-operation with national data protection authorities. The European Data Protection Supervisor will, for this purpose, replace the Schengen Joint Supervisory Authority. Individual data protection rights have been secured, such as the right to information for the data subject where now specific information is provided for that purpose. Regarding the operational management of SIS II we believe that the solution found by the co-legislators is consistent with the Community's approach because in the first instance management will be carried out by the Commission and in the second phase, after a thorough debate, one of the options, and the one we tend to favour at this stage, will be the devolution of this responsibility to a European agency.

Q389 ***Lord Avebury:*** Are these amendments that you have just been talking about incorporated in a consolidated text or is that still to be published?
Mr Faull: Yes, there is a consolidated text now.

Q390 ***Lord Avebury:*** Since the 23 November meeting of the Parliament?
Mrs Boulanger: There is no formal adoption of the text yet. I do not know exactly what is published yet but the adopted text will incorporate all the points that have been mentioned by Mr Jonathan Faull.

Q391 ***Lord Avebury:*** Could we have a copy of that, do you think?
Mr Faull: It is a matter for the Council Secretariat, not for me, but I am sure one can see what can be done.
Chairman: Thank you very much indeed.

Q392 ***Baroness Bonham-Carter of Yarnbury:*** Picking up on what you were just saying, originally, according to your paper of 28 July, you proposed that the Commission should be responsible to ensure continuity between development and operation of SIS II. Why do you think so many Member States are so insistent that it be devolved to an agency? How would you assess the Commission's record of managing the SIS II project up to this date?
Mr Faull: Overall I think we are reasonably satisfied with the way the project is going. We regret that it has been necessary to reschedule because of delays that have occurred. They have caused frustration, and a lot of political concern particularly in the new Member States of the Union. Most of the causes of delay, and I am happy to go into them in detail if you like, have been outside our control and I have to say that they are not uncommon in very complex projects of this sort in Member States and elsewhere in the world. This is a very complex, large-scale IT project involving a whole set of national systems as

well as the central system. There is a great deal of effort made to co-ordinate the progress of the national projects and the central European project. We have two sites, one in Strasbourg and a back-up site near Salzburg in Austria. Frankly, my Directorate-General is still a rather small one in the scheme of Commission things. Where we have perhaps failed to exercise supervision as well as we could, has been in our relations with the main contractor for the central system where there were some delays and we regret that very much. We also had a bout of litigation against various awards of contracts, both in my Directorate-General and another Directorate-General of the Commission responsible for a network that we have to use and there has been litigation in Member States. Again, this is not unusual as these are large, rather juicy contracts. The bidders who are not successful in getting the contract often go to court and even if cases are won or settled at the end of the day, as they were, there are delays. All of those things, I am afraid, occurred and therefore a certain amount of delay, not of extraordinary proportions but a certain amount of delay, has occurred and we have therefore rescheduled the project. When I say "we", essentially the Member States came to an agreement on a new schedule for the project. They, by the way, took advantage of that rescheduling process to add further months on for their own testing purposes back at home. I think by its very nature this is a project where a certain amount of learning takes place in doing. The project has changed in nature in its short life. The computer specialists working on it, both at our level and at the Member State level, came up with new ideas, discovered new problems, asked for changes in the way things were being done, a lot of the time perfectly reasonably, and we had no problem in giving our consent to that, but sometimes things were speeded up and sometimes they were not. For all of these reasons there has been delay and it is regrettable. I do not think that the Commission's management of the project, and please remember that the Commission's management is limited to the central part of it which is only one section of a much wider set of projects, has been called into question to the extent that people want to rush to an agency to implement the project immediately. The agency idea is certainly a very important one, and has our favour for that matter, for subsequent stages of this project once it is up and running. The important thing now is to get it ready so that the central system is ready to "go live", as we say, the national systems are ready to plug into it, the old systems adapting to it and the new Member State systems newly created for that purpose, and then once we have completed the Schengen evaluation inspections and reports in the candidate countries for full membership of Schengen the Council will be able to take the political decision to lift the internal borders.

Q393 ***Baroness Bonham-Carter of Yarnbury:*** But the agency was not your preference?
Mr Faull: The agency is not our preference at this stage of the project, no.

Q394 ***Baroness Bonham-Carter of Yarnbury:*** Can I just ask you one thing about the litigations that have held things up which you mentioned. As I understand it, those were about a perceived lack of transparency in the tender process. Would you accept that?
Mr Faull: That was one of the arguments in one of the cases, which is not uncommon.

Q395 ***Baroness Bonham-Carter of Yarnbury:*** Is that something you regret?
Mr Faull: No. We had very good arguments to respond to that allegation and we believe that we complied fully with all the requirements in the procurement process.
Dr Paul: May I add something as regards the reasons for the delay. As the Director-General mentioned, at times there has been a temporary lack of performance or a slight under-performance by the main contractor and an internal audit found had we supervised the contract better then probably this under-performance would not have happened. At the same time, the audit very clearly conceded, as was indicated in the audit statement, that there was a structural under-staffing and with the level of staffing we had at the time we could not properly supervise the contract. What is very important is to point out that under-performance in itself did not cause the delay. The delay in the SIS II project was triggered by the inability of the French administration to prepare the site on time. That triggered the delay and then led to a broader discussion about the rescheduling of the project and it was then that Member State experts said, "Yes, and by the way we also need much more time for testing our own systems". There is not a single expert from Member States who has told us they need less time; on the contrary, some of them insist even until today that they would very much like to have more time to implement the national systems.
Chairman: I think Lady Bonham-Carter may want to move on to another question but can I first ask Lord Teverson to come in.

Q396 ***Lord Teverson:*** I should explain to you that I am new to this Committee. I would like to ask a rather more question on the question of delay. Schengen became part of the Acquis in 1999 and by 1999 we already knew that the regatta approach to accession of new Member States was going to stop

and all ten were going to join in around 2004 and we knew that Schengen I could only cope with 18 Member States, so in some ways we have had getting on for eight years to prepare for this now. From a general strategic point of view, and this is not particularly a Commission point but more a broader EU issue, I do not understand why we are where we are at the moment given the fact that we knew we would be where we are eight years ago.
Mr Faull: Thinking back to 1999 I am not sure that we did know that ten Member States would join in 2004. It is true that the regatta approach was beginning to fray and political decisions perhaps were already being prepared for a big bang, but I do not think it was clear enough—I was doing something completely different then—for serious planning for Schengen expansion to begin immediately. I think that would have been premature. Nevertheless, I take your general point that this was a challenge that was bound to come and the earlier we started planning for it, all of us, the better, there is no doubt about that. All I can say is we started when we thought it was reasonably necessary and prudent to do so. We realised from the outset that this was a project of considerable technical, economic, political, legal complexity and magnitude and perhaps we did not anticipate all the obstacles which we would have to jump over or get round, but we thought very hard about what most of them would be and tried to devise solutions. I think we expected the legal basis instruments to be ready earlier than they were. Because it is in the nature of these large procurement projects, we expected someone to sue somebody at some stage, but you never know when and where and how and what the outcome will be, so you cannot provide for all eventualities. Frankly, we did not expect to have the problems we encountered on the French site with the preparatory work, and it came down to such basic issues as getting the air conditioning right because these are massive computers requiring climate control. We did not expect to have the difficulties we have had there just as we are still surprised to be facing problems today, frankly, about the provision of some of the data needed for the tests to be carried out which in turn will provide either confirmation that everything is right or additional problems to be solved in the detailed design of the system. As I speak to you today we are still waiting for the French managers of the C.CIS system down in Strasbourg to provide some of the data necessary for testing purposes and we have not got them. Yes, there are some unforeseen problems that one may say we should have worked harder to anticipate. I think we anticipated as much as we could but this was always going to be a lengthy project. I regret that it is a little lengthier than we originally thought it would be but it will be delivered pretty soon. We all recall the SIS I system which we have all got used to and seems to be working so happily: that was how many years late?
Dr Paul: Three years.
Mr Faull: Three years late all those years ago. We are not complacent and any day's delay is regretted but we will get SIS II up and running very soon.

Q397 ***Earl of Caithness:*** I would like to take you back to some of the court cases, in particular the *Cap Gemini* case where the ECR said that "*prima facie* the Commission committed a manifest error of assessment in awarding the tender". Would you like to comment on that, please?
Mr Faull: We believe we had very good arguments for rebutting that *prima facie* finding by the court. The President of the Court has to make a *prima facie* finding as one of the conditions for issuing an injunction. We had good arguments against that. They were never tested in court because, as you know, the case was settled and withdrawn.
Chairman: The next question was going to be about delays but, if I may say so, you have given us a very comprehensive and persuasive answer.

Q398 ***Earl of Caithness:*** Can I ask a supplementary on delays. Could you tell me what the update position is with regard to the claim by various countries like Poland and the Czech Republic for compensation from the Commission for the delays and being treated like second-class citizens?
Mr Faull: Nobody has been treated like a second-class citizen.

Q399 ***Earl of Caithness:*** That is what the Czechs say.
Mr Faull: I know. I am afraid there are allegations but they are not founded. I regret very much that political perception which I have to acknowledge is out there. The effort to be made here and there to bring the new Member States, Poland, the Czech Republic for example, into the Schengen System is a considerable one. We are making that effort and I am sure the Poles and the Czechs are making that effort. There have been delays in Poland and the Czech Republic, there have been delays elsewhere and there have been delays centrally and they are all to be regretted. I do not think there is any intention on anybody's part to treat any Member State differently from any other. Our only role in this is to enable the Council to make the decision on lifting the internal borders as soon as possible knowing that the conditions in the SIS II system, which is so essential for our security and for law enforcement within the Schengen area, are properly in place. That is our responsibility, we are doing that. We are not getting into name calling or blaming and shaming. There have been delays in various places

but all Member States wanting to join the Schengen area should have an opportunity to do so as soon as all the appropriate conditions are met.
Chairman: Thank you very much indeed. I think we should move on to biometrics.

Q400 ***Baroness Henig:*** We are moving forward now. I would like to ask what is the timetable and likely content of all the measures implementing the Schengen II legislation which the Commission must adopt, including the standards relating to the use of biometrics.
Mr Faull: There will be implementing measures to complete the SIS II legal framework. We will produce those implementing measures, including those relating to standards for the use of biometrics, and a new SIRENE manual. Can somebody remind me what SIRENE stands for?
Mrs Boulanger: It is Supplementary Information Request at National Entry. In practice the acronym does not reveal the content exactly.
Mr Faull: Anyway, there will be a new version of that.

Q401 ***Chairman:*** I think we call it *sirène*, do we not?
Mrs Boulanger: Yes.
Mr Faull: It sounds odd in English, does it not? All of that will be necessary for the proper application of the legislative instruments and for SIS II to start operations properly. According to the rescheduling agreement reached in the Council in October these measures should be adopted by August 2007 which will leave enough time for the Member States to provide for internal measures to implement them before SIS II moves into its operational phase. They may need subsequently to be amended further when biometric searches start since those biometric searches will in turn depend on the availability of the proper infrastructure at the central site and the readiness of the Member States to set in place the requisite training of the people concerned, the equipment at a national level and so on.

Q402 ***Baroness Henig:*** What is the likely timetable and content of the Commission report on the use of one-to-many biometric searches?
Mr Faull: I am just checking my notes.

Q403 ***Chairman:*** I am sorry, I think this is an unscripted question.
Mr Faull: All right then, Frank. He is better at improvising than I am.
Dr Paul: It is very clear that the biometric search capacity will only be introduced once the system is up and running. That has been made very clear from the outset. When that time will be depends very much on when the Member States will be ready to transmit such information and do the searches having done the training of all police forces, et cetera. When this will happen will depend on the final timeframe for making the SIS II operational. You will probably know that for the time being Member States are discussing in the Council the possibility to temporarily enlarge the current SIS I system to a system called SIS one4all. That is the name that has been given to this initiative by the Portuguese Government which initially suggested this idea. If it is decided by the Council on 4 and 5 December that Member States will go for that option, and thus new Member States will be integrated into the current SIS I, this will inevitably have a repercussion on the timing for the SIS II, so there will be further delays in making the SIS II available if that initiative is implemented. It really depends on the time when the SIS II is made available. We estimate the time that is needed to implement the biometric search functionality in the SIS II once it has become operational is probably something about two years, but again very much depending on the ability of Member States to perform these biometric searches. It goes without saying that we will of course look at this very closely both from a technical and data protection point of view. The way we will do this is probably link it to the infrastructure of the so-called biometric matching system which is a service oriented architecture that will serve simultaneously various applications, such as the VIS—the Visa Information System—and then the SIS II.

Q404 ***Baroness Henig:*** When you have done all that and you have presumably reported on that some time down the line, how can the Commission ensure that your report is acted on by the Council?
Dr Paul: I did not quite get the last bit.

Q405 ***Baroness Henig:*** You have been describing the process as somewhat down the line that you, as the Commission will oversee what is going on and presumably report on this at some stage.
Dr Paul: Yes.

Q406 ***Baroness Henig:*** How can you then ensure that your report is acted on by the Council at that point in time when you have done that?
Dr Paul: There is no further need for a specific legal instrument to be adopted. There will be no further consultation of the European Parliament on a new legal instrument, for instance, we will just implement it as we have foreseen according to the then established standards that still need to be studied when we are ready to implement biometrics.

Q407 ***Baroness Henig:*** So you will just go ahead and it will not go to Council at that stage.

Dr Paul: We will report to Council and the Parliament.
Mrs Boulanger: The Commission will prepare a report and the report will be submitted to the Council and the Parliament.

Q408 ***Baroness Henig:*** How will you then ensure that it is acted upon?
Dr Paul: This is the point. There will be no further legal act that would involve Parliament to implement the biometrics. If you refer to the authorisation to implement, this has already been given in the currently adopted legal instrument.
Mrs Boulanger: If you will allow me to add something. Most probably this would be done via the comitology procedure and, as you know, all the acts the Commission adopts via the comitology procedure are transmitted to the Parliament, so the Parliament has some rights according to this procedure.

Q409 ***Lord Teverson:*** Can I ask for clarification. Forgive me if I have not been listening properly. Are you saying, which I had not picked up, that there is now a Portuguese proposal that SIS I be extended in order to take in new Member States which would then have priority over the development of SIS II so it moves forward the political objective of integration of the new Member States and then we deal with SIS II?
Mr Faull: The Portuguese have proposed a system whereby the SIS I could be cloned, in effect, and made available for the new Member States immediately, solving the capacity problem, at least in the short-term, but not adding on any new features. That is currently being discussed and will be discussed again in the Council next week. Member States are somewhat divided on the issue. Obviously there is a resource issue, particularly in the smaller Member States, where we have alerted people to the danger that by working now on SIS I they will essentially cannibalise the teams working on SIS II because they are not going to find extra people that easily, so this will add a further delay to the SIS II project which meanwhile everybody says remains fully necessary. The political attraction of finding a quick fix and dealing with the second-class citizen perception that the Earl of Caithness referred to is powerful and one has to acknowledge that. It may release some political pressure now but whether it will fulfil all the expectations is very much a matter of discussion. I understand that the Member States met in the Article 36 Committee to discuss this yesterday and it will be discussed by the Permanent Representatives Committee, Coreper tomorrow.

Q410 ***Chairman:*** Do you know if it got much support yesterday?
Mr Faull: I think it got some support. I do not know whether my British friends sitting over there were present; I was not. Were you, Marie-Hélène?
Dr Paul: I was present.
Mr Faull: You were present, Frank. I had a very quick read-out just coming over here this morning from Frank, and he can add something. There is some support but considerable division still. Is that a fair characterisation?
Dr Paul: Yes, it is a fair characterisation, however I would say at this stage the probability of this being adopted remains relatively high.

Q411 ***Chairman:*** High?
Dr Paul: Yes, relatively high. That said, if you will allow me to come back to the question you have just put, I understood from what you said that you think this indicates a priority that is given to the SIS I-for-all project over the SIS II project.

Q412 ***Lord Teverson:*** Only from what Jonathan was saying himself.
Dr Paul: In theory, at least, equal priority will be given to the SIS II and the SIS one4all projects. The delay that I was referring to is caused by the risks Mr Faull quite rightly underlined. However, it is also a purely and absolutely inevitable technical consequence. The reason is simply that under the current development plan for the SIS II we would have to migrate the 15 existing users, the 15 existing Member States, from the old system into the new system. If the new Member States are integrating into the old system it automatically increases the number of Member States that would have to migrate and it takes a certain amount of time for each Member State which leads to those inevitable delays. The delay is of a simply inevitable technical nature.
Mr Faull: May I make an off the record comment?

Q413 ***Chairman:*** Please.
Mr Faull: (The answer was given off the record)

Q414 ***Earl of Listowel:*** Director-General, can you provide some help in explaining why are none of the measures that you have been discussing subject to the new "regulatory procedure with scrutiny", and this is a procedure which gives control over draft implementing measures to the European Parliament? Is any part of these implementing measures likely to be secret?
Mr Faull: The regulatory procedure with scrutiny, which is a quasi-legislative procedure, was considered unsuitable in this case because the implementing measures we are talking about are not intended to amend or to supplement the legal

instruments themselves. They are technical or operational implementation of what has been agreed in the legislation rather than implementation of such a nature as basically to amend the original legislation. The adoption of the implementing measures by the Commission will, we believe, constitute a step forward in comparison with the current SIS arrangements in transparency terms where, frankly, some implementing measures are not formally established at all, things are done, agreed by the technical people involved, and, if reduced to writing at all certainly not made available. In accordance with comitology procedures we will send to the European Parliament all the draft implementing measures we are speaking of and they will be available to the public in accordance with our normal document access procedures.

Q415 ***Lord Teverson:*** Director-General, this is around the proposals on the management of SIS II and what options there are available. We are particularly interested is one of those options the management of SIS II by agencies like Europol or Frontex or an existing organisation within the EU family?
Mr Faull: We have started work on what will be a major impact assessment on the long-term management of SIS II and we will also encompass in that the other large-scale IT systems that have been created in the justice, freedom and security area for which Frank Paul is responsible. We do not know what the impact assessment will say obviously, but we have identified five options which we think are worthy at least of consideration: a brand new agency; the Frontex agency, the agency for the management of the external borders which lives in Warsaw; management by the Commission which could either be direct or delegated management by an executive agency but under the Commission's aegis; management by Europol or management by a Member State on behalf of all the others. All of those things are possible, they have merits and they have demerits. We will look into them and provide the best objective arguments we can so there can be a proper debate and then a decision on them. Another option to be considered is whether we are talking only about SIS II or whether we would include in a package the other big computer systems that have grown up in the justice and home affairs areas and which there is a fairly widespread school of thought that it is not the Commission's usual core business to manage.

Q416 ***Lord Teverson:*** Could I ask out of my ignorance how that decision is made? Who makes that decision? What is the procedure?
Mr Faull: It would require legislation.

Q417 ***Lord Teverson:*** It is a legislative issue?
Mr Faull: Yes.

Q418 ***Lord Avebury:*** Before asking my next question can I ask a supplementary on that one. Are there not strong management arguments for allocating this to an agency which already has experience of large-scale computer system management? In that sense would not, for example, Europol be high on the priority list rather than establishing a new agency which has to acquire the capability of managing large computer systems from scratch?
Mr Faull: In general I am sure you have a very good point that if we have an agency with successful experience of managing large-scale computer systems they will have developed skills, experience and expertise in systems which would encourage the view that they should at least have a shot in this context as well rather than starting everything from scratch. That is a compelling argument.

Q419 ***Lord Avebury:*** The five alternatives that you mentioned, will these be evaluated from the cost point of view so that you can differentiate between those who do not need large-scale training programmes for completely unskilled or inexperienced staff?
Mr Faull: Very much so.

Q420 ***Baroness Bonham-Carter of Yarnbury:*** Can I put something to Dr Paul. One of the things when I listen to this is, and this is a very basic question, are you concerned about the co-ordination across all these different IT systems, all these different countries? Picking up on what Lord Teverson was saying, if you have got this cloned SIS-plus, or whatever it is called, coming into the middle of your plans, and it sounds to me like throwing off what you have been concentrating on, is there a real concern that this co-ordination of systems will be achieved?
Dr Paul: Generally speaking, as regards the future management of the system, and that includes the co-ordination, the Commission adopted at the end of 2005, December 2005, a communication on possible synergies when managing large-scale European databases, including the SIS II, the VIS and EURODAC and any other systems that might emerge in our area. This clearly outlined a number of options and issues which are up for discussion with Member States now as to how to achieve a maximum of synergy and simply very efficient management of those systems to avoid those co-ordination issues that you have mentioned. Unfortunately, up to now the subsequent presidencies have not really taken up the issues that were pointed out in this Communication. We hope that this is going to happen very soon now

because we have to move forward with this issue. As regards your question relating to the SIS one4all, this project will be managed by the Portuguese administration if it is adopted, of course, and the technical management will continue to happen at the C.SIS in Strasbourg which means the French administration mandated by the Member States. Legally speaking and, indeed, operationally speaking the Commission would not be involved in this SIS one4all project. Of course, speaking overall, especially at national level, the co-ordination will become more difficult and there will be an issue of resources to do the two things in parallel.

Q421 ***Lord Avebury:*** Coming back to the question that I was down to ask initially, can I ask about the power to adopt implementing rules. Will they already have been settled prior to the appointment of the agency or will the agency that manages SIS II have the right and the power to adopt its own implementing rules? Secondly, could you tell us what mechanisms will be adopted to ensure the future accountability of whatever agency is appointed to run SIS II?
Mr Faull: That is a very important question and it is one which arises frequently when agencies are created. Agencies cannot be given rule making or law making powers. The legislature remains responsible for that or, under delegated authority, the Commission and various comitology procedures, as you know, have been created to regulate all of that. What we cannot do is cede any discretionary policy-making power, let alone legislative authority, to an agency. All that said, and that is the legal position which should not surprise anybody, for an agency to operate particularly in a complex area like this it needs some margin for the taking of decisions to deal with issues that arise. The legislation creating it, therefore, has to be designed carefully so that all foreseeable eventualities are dealt with in some way and rules are laid down very clearly while allowing the agency to grow and deal with such issues as it can when they arise. We will go again into all of this in the impact assessment. It is indeed one of the issues relevant to the question whether an agency is the right solution. Can you craft an agency which can do this job properly? Frankly, I do not know the answer to that today. The whole process of impact assessment and then deliberation will help us answer it. I hope it is possible because I think these are important options which should not be discarded and I hope they are still in the race towards the end, but we will have to see. It is difficult but ways can be found to create a clear enough legislative framework so that the rules are made by the people with the authority to make them and with the democratic legitimacy required to make them, and the agency is given enough space in which to do its work on a day-to-day basis. It is not easy to do, it is a problem which all countries face as well as the Union as a whole, but we have all found ways to deal with the issue in the past. Frank, do you want to add anything to that?
Dr Paul: Not necessarily, although if you will allow me I would like to come back to the question that was put earlier by Lord Teverson. I understood your question as meaning why has there not been enough strategic forward planning when developing the SIS II, is that correct?

Q422 ***Lord Teverson:*** That is very concisely correct.
Dr Paul: I think it is important to recall, and I was there at the time, that this was an historic development moving from the intergovernmental management to Community management. Indeed, the problem was that as early as 1996–97 it was seen that the current system would have some technical limitations, at least then it had technical limitations, which would not enable it to be enlarged to more than 18 Member States. It was already clear then that the European Union would be enlarged by more Member States. There was a very, very long and intensive discussion among Member States that lasted about five years on how to solve this issue. At the time Member States were very reluctant to entrust that enlargement to one single Member State, namely France, because it was already clear that eventually the system would move into the Community framework. It took Member States a long, long time to discuss this and at the end of the day it became clear that there was no other solution than to simply entrust the Commission with doing it because nobody could get agreement on who would do it. Therefore, we only got the mandate to develop the SIS II at the end of 2001. From then on we have moved as fast as we could possibly move. If you take a look at the history of large-scale IT systems, you might want to look at your own National Health System IT system, for example, these are complex systems.

Q423 ***Chairman:*** We might indeed!
Dr Paul: These are complex systems that take many years to develop. As large-scale IT systems go we have always worked to a very challenging timeframe.

Q424 ***Chairman:*** I should just say on a personal level I have an unhappy history of a relationship with IT systems, but we will not go into that.
Mr Faull: I do not think I fully answered the question about the role of the European Parliament and the accountability of an agency, again an issue which frequently arises in the whole area. We have comitology, we should have "agency-ology" as well, I think! The impact assessment will go into that. The role of the Parliament is important in all of the

options we will consider and the Parliament would remind us of that if we were ever tempted to forget it, which we will not be. The role of the Council and Parliament in establishing the agency, in choosing its members, its chair and in supervising it, will be extremely important issues. Some of you will be familiar with the process we are agonisingly going through to set up a Fundamental Rights Agency at the moment and those issues are, once again, at the heart of one of the major debates about precisely how this agency should be created, to whom it should report, who is responsible for choosing its members and so on. These are very important questions.

Q425 ***Baroness Bonham-Carter of Yarnbury:*** Another accountability question. The Commission has the possibility, as I understand it, to delegate its management of SIS II to Member States for a transitional period. Is this likely to happen? If so, how will the financial and legal accountability of those Member States be ensured, including as regards data protection?
Mr Faull: Yes, indeed it is a very real possibility and the legislation makes that clear. The Commission would retain overall responsibility and would have to enforce strict compliance and control mechanisms under our financial regulation. We would have to set out in agreement between the Commission and the national bodies concerned all of the complex set of arrangements on legal, financial issues plus on accountability and transparency issues. We would certainly place them very high on our agenda and would want to be sure that the delegation of certain tasks to national bodies in that way would not undermine the roles of the Court of Justice, the Court of Auditors and the European Data Protection Supervisor, to name but a few. This would be a matter of negotiation and agreement between the Commission and the national authorities, and I can assure you that uppermost in our minds would be the issue of proper supervision and accountability.

Q426 ***Baroness Bonham-Carter of Yarnbury:*** Is this process a result of pressure from Member States? What is behind it?
Mr Faull: Well, no doubt some Member States think this is a good idea but we ourselves see merit in it as well. We have to use the experience that some of our national authorities have built up and where it makes sense for some sort of joint venture of this sort between the Community level and the national level to be set up, why not?

Q427 ***Earl of Caithness:*** Does the Commission believe that there are any circumstances in which the UK should have access to alerts concerning non-admission of third country nationals, for example access for asylum purposes, or access only to alerts concerning persons subjected to an alert because of criminal convictions or alleged criminal activities? If so, how should that access be regulated?
Mr Faull: As the United Kingdom does not participate in policy areas linked to alerts for the purpose of refusing entry it is not as a general rule to have access to those data. In my written evidence on the question of access for asylum authorities, I said that an ad hoc solution allowing indirect access for UK authorities could be examined once the legal instruments, including provision on access rights, have been adopted. There has been some preliminary discussion among the Member States with the Commission on this issue. The principles of proportionality and reciprocity would be at the heart of any such examination.

Q428 ***Earl of Caithness:*** Would it not be a good thing for Europe if the UK did have access to some of the information in exactly the same way as it would be good for the Schengen countries to have access to some of the UK information? Surely if we are paying our full share, why are we not given access?
Mr Faull: We believe that there are indeed good arguments for believing there is mutual benefit among the Schengen members on the one hand, and on the other the United Kingdom and Ireland, in sharing some information. We believe it would be of greater benefit to Europe if the Schengen area extended to the whole of the European Union but we understand at the moment that is not on the agenda. This is not simply a case of the United Kingdom seeking to have its cake and eat it, and I do not think the other Member States see it in that simplistic light either. The United Kingdom and Ireland have contributions to make to the overall security of the European Union and the others, I believe, through the Schengen Information System have contributions to make to the security of the United Kingdom and Ireland. Ways have been found in the past pragmatically to square these circles. As I said in my written evidence, by making the proper distinction between the uses to which information is put ad hoc solutions can be found.

Q429 ***Lord Dubs:*** Can I ask a supplementary. I think that is very encouraging because we accept that not being in the club means we are not entitled to the benefits of the club, but I think this is rather different, this is a matter of dealing with possibly the link between criminal behaviour and movement across frontiers. Therefore, I would have thought that the Schengen countries have as much to benefit from as the UK if what you suggest were to happen. How likely is it to happen?
Mr Faull: That is hard to predict and I do not really want to speculate. What I can say is that I think there is a perception in many quarters of the sort that you

have described and there is mutual benefit. The United Kingdom, not being part of the Schengen, area should not have information relating to entry for the sole purpose of regulating entry because the United Kingdom has other arrangements in place regarding entry to its territory, but the wider security implications of some of this information need to be taken into account. I cannot tell you how this will come out but based on the past record I think there is some evidence that there is understanding of that position in London and also in continental capitals as well.

Chairman: That is very helpful. I think I can confidently say that the implications of the partial opt-in or partial opt-out, depending on whether the glass is half full or half empty, for both the United Kingdom and Schengen countries will be an important part of our report and your explanation has been extremely helpful for us.

Q430 ***Lord Dubs:*** What is the timetable for, and likely content of, further SIS II proposals concerning the harmonisation of alerts for non-admission of third country nationals, the rules on "flagging" certain criminal law and policing alerts, and the rules on remedies in the context of data protection? I know it is a mouthful.

Mr Faull: I understand. We have to make an assessment within three years of what is called the go-live decision which is essentially when the SIS II system is plugged in and the existing Schengen countries can plug into it and the new Member States can be integrated into it. Within three years of go-live—my colleagues should correct me if I get this wrong, it is technical—we have to assess the impact of the new legal rules and evaluate the urgency with which a review should be carried out and the scale of the review to be carried out in order to see whether a further higher level of harmonisation is necessary and appropriate. We will do that exercise within three years of go-live.

Q431 ***Baroness Henig:*** In the light of the judgment in *Commission v Spain*, is the Commission still monitoring the use of Schengen data by all Member States to ensure that no Member States breach EC free movement law or immigration or asylum law when they act upon an alert? Is the Commission also monitoring the issuing of alerts by Member States?

Mr Faull: First of all, if there are complaints about failure to comply with Directive 2004/38 we of course take them very seriously. If there are complaints about refusal of entry or refusal of visas because of issues arising under that Directive we look at them very carefully as well and use both our informal powers of persuasion and formal powers to bring infringement proceedings against Member States where necessary. We also have an alternative dispute resolution mechanism known as SOLVIT, which is run by our Internal Market Directorate-General but we are associated with it for areas under our responsibility. It seeks to resolve very quickly problems in individual cases by asking the national authorities to move quickly. Overall that is a very satisfactory system and is often used as a preliminary phase before the lodging of a formal complaint which then triggers more formal proceedings.

Q432 ***Earl of Listowel:*** Director-General, in relation to SIS is any information available on the number of complaints made about inaccurate data and other exercises of data protection rights?

Mr Faull: We do not have those data. The Joint Supervisory Authority, or perhaps the national data protection authorities, would have them. From what we know it appears that the number of complaints is very small in comparison with the number of alerts stored in the SIS, but we do not have a figure. Is that right?

Dr Paul: No, we do not.

Q433 ***Lord Teverson:*** The Treaty of Prüm, which is again a group of Member States moving off in their own way, and we understand the German Presidency would like to see a movement towards that becoming part of the wider Community Acquis, what implications would that have for SIS II? Indeed, is the Commission in favour of this happening?

Mr Faull: Yes, we are. We believe that the general Community interest would be well served by bringing the Prüm system into the Community's institutional framework and, therefore, we support the intentions of the German Presidency and will work with them to that end. We think that the Treaty of Prüm does not conflict with the scope and objectives of SIS II. In fact, it is consistent with them regarding the implementation of the principle of availability which was laid down in The Hague programme by the European Council. We have asked the incoming German Presidency to make sure that discussions on bringing Prüm into the Community fold are accompanied by discussions on implementation of the principle of availability. We note that the data protection system of the Treaty of Prüm is tailored specifically, of course not surprisingly, for that Treaty and we have no objections to the way in which that was done.

Q434 ***Lord Teverson:*** Could I just interrupt you. Excuse me again for my lack of knowledge, but could you explain the principle of availability to me.

Mr Faull: The principle of availability at the most general level says that information held by or for a law enforcement authority in a Member State should be made available to the law enforcement authorities of other Member States on the same conditions as

those which would apply to making the information available to the law enforcement authority of the first Member State. That is terribly long-winded but you understand what I mean, It is national treatment. It is so general that everybody agrees to it. It is difficult to work out in practice although we are beginning to do that. It has a number of fairly wide-ranging implications, including that information which looks national or even local may be potentially of interest to law enforcement authorities in other Member States. We believe that is the case and that has a number of consequences for the way in which that information is dealt with. That brings me to data protection. One of the problems we have, and Prüm deals with it within its circumscribed scope, is the Union needs a data protection system for the third pillar as long as it remains in place, and the Council is busy working on a proposal for the establishment of a data protection framework decision, which is what Directives called the third pillar to simplify, and we hope very much that the German Presidency will carry that forward and, indeed, secure its adoption by the end of its term in office next year.

Q435 ***Chairman:*** I think it is not irrelevant to this discussion to draw your attention to a report which this Committee produced on the Heiligendamm meeting, that is to say addressing both the accessibility and transparency of decisions taken by a limited number of Member States and the extent to which that applies to the whole European Union. I have just been prompted to ask you a supplementary question on that issue. As a general matter, does the Commission think that a number of Member States agreeing on their own legislation and then exporting it to the rest of the EU is a good way of legislating? If that is not a question expecting the answer "yes" or "no", I do not know what is.
Mr Faull: Can I give a more long-winded answer?

Q436 ***Chairman:*** Would you.
Mr Faull: First of all, let me say that we read with great interest your report on Heiligendamm and it was much cited and commented on and I think was a great credit to your Committee.

Q437 ***Chairman:*** Thank you.
Mr Faull: The best way to legislate in the European Union is for the Commission to make a proposal, the Council and the Parliament to co-legislate and the Court of Justice to adjudicate. That is the good old Community method and we believe that it has served us all well in many areas and has proved robust enough to work in this area as well in perhaps surprisingly successful circumstances. The Data Retention Directive, which the British Presidency did so much to adopt, is a very fine example. We know that there are other ways in which the Union moves forward and one way we have to accept is for groups of Member States to establish an idea which hardens into rules of some sort and which eventually come home into the Community fold. There is nothing necessarily automatic and determinist about that but that is what happened with Schengen, which is why we are here today. Schengen was the dream of Luxembourg and its neighbours to start with and that is why it bears the name of this now very famous village at the borders of Luxembourg, France and Germany.

Q438 ***Chairman:*** Where I have quite frequently lunched.
Mr Faull: Have you? The local wine is very good. Now it is probably the most famous place in Europe. It is spoken of around the world in the same breath as London, Paris, Caithness, Richmond and various other places.

Q439 ***Chairman:*** Nothing to do with my lunches!
Mr Faull: It is an example. It is an example that predated the Europe of 27. There is a certain tendency to say that with 27 Member States you are bound to have groups of Member States coming together because of their geographical locations or because of their perception of their size or whatever to do things together. I do not think there is anything inevitable about it. I think the Europe of 27 can be made to work and it does work most of the time, but I also know that long before we were 27 we had cases in which smaller groups of Member States did something which appeared to them to be in their local interest to start with and then others saw would have benefits for everybody else and they all saw together that the best way to run things in the European Union was to use the institutions which have been created for that purpose.

Q440 ***Chairman:*** The northern dimension is a very good example which was discussed in Helsinki last week.
Mr Faull: Exactly. There is a northern dimension, there is a southern dimension and there is an eastern dimension. The Mediterranean countries have problems which are not the same all the time as those faced by the Nordic countries, and that obviously makes sense. There I think one does see the expansion of the Union at play. Nevertheless, most of the big issues and challenges we face when we look at the wider world are common to us all and that is why I believe that most of the time the European institutions are the ones which work and should be used. I have no dogmatic objection to the practice of groups of Member States meeting to talk about operational matters and, indeed, to begin talking about rules which one day can become Community rules. There are all sorts of issues which you

highlighted in your report about accountability and transparency. We may be criticised in the authentic institutional framework for some of our shortcomings in transparency and accountability but at least we have rules. They may not always be the right ones, they may not always be fully complied with, in which case you should rap us over the knuckles, but we have them, some of these groups do not really have them and clearly that is an issue which may cause concern. We are generally of the view that the institutions are well tested and should be made to work by all concerned. If good ideas come from elsewhere we are not proud, we will consider them, and if they are the right ones we will seek to extend them to everybody else.

Q441 ***Lord Teverson:*** Forgive me, Director, if I could come back to the Portuguese issue again. If SIS I is extended in terms of numbers of Member States it can cope with then is there not a temptation, if that has been achieved, that you just bolt-on the extra information fields in terms of biometric information on to that SIS I system? You have taken away the political momentum in terms of SIS II so to avoid all the issues of systems development that we have talked about is there not a temptation just to add another bit on that gets over the problem altogether?
Dr Paul: Technically that is simply not possible. The big advantage of SIS II is that it provides more flexibility, it is more easily scaleable, et cetera, whereas SIS I dates back in its architectural conception to the early 1990s which in terms of IT is really the Stone Age. We are now moving towards a much more flexible system and it would simply be impossible to incorporate any biometrics in the present system. If you want the new functionalities, there is no choice. That is also interlinking alerts, which is very important to be more efficient in finding people and solving crimes. There is no choice but to move to a more flexible system and SIS II will provide exactly that.

Q442 ***Lord Avebury:*** You talk about the Prüm system being brought into the framework of European law together with its own data protection regime that applies to it and at the same time in parallel you have got the DPFD being developed to correspond with the principle of availability. Is it not going to be extremely confusing to have more than one data protection regime applying to similar types of data? Would not the logical outcome of bringing the Prüm Treaty into European law be to apply the DPFD to its provisions as well?
Mr Faull: Yes, you are absolutely right, it would be vastly preferable to have one system that everybody can operate and live with. It comes down to a question of timing: will the data protection Framework Decision be in place when Prüm comes in? I do not know. We do not know precisely when the Framework Decision will be adopted and we do not know how the domestication of Prüm will work in timing terms either. It is better to have some data protection than none at all but ultimately the whole thrust of our proposal for the Framework Decision is that there should be one universal regime, if you like, for data protection in third pillar issues.
Chairman: Director-General, we have imposed on your time and generosity. I think there is one quick supplementary question from Lord Listowel to which we invite a quick reply.

Q443 ***Earl of Listowel:*** I would be very grateful if you did have time to answer this question. I apologise for not giving you notice in writing beforehand. The Hague Programme indicated that there will be a proposal from the Commission to supplement the existing Schengen evaluations with a supervisory mechanism ensuring the full involvement of Member States' experts and including unannounced inspections. Could you tell us more about this? This was a particular concern raised by the Deputy Information Commissioner in our country about the monitoring process rather than the evaluation before. If you prefer to write to me after the Committee that would be very welcome.
Mr Faull: I will. What I can tell you immediately is that we have not yet made that proposal. I will very happily write to you and tell you exactly where we stand in the preparation. I do not think very far because it has not crossed my desk.

Q444 ***Chairman:*** Director-General, when you see the transcript if there are other things that you think will be helpful for us for you to follow up in writing we would be very grateful if you would send it to us. May I express warm gratitude for the way in which all three of you have dealt with our questions. It is very nice to have seen you again. I have no doubt that this Committee will have further contact with you and your Directorate-General. Thank you very much, and again thank you for coming here to give your evidence. It has been very nice to see the three of you.
Mr Faull: I should perhaps disclose that I shall spend this afternoon in the company of colleagues of yours from the other place.
Chairman: Indeed. Word had reached us to that effect. Can I wish you and them good luck. Thank you very much.

28 November 2006

Supplementary written evidence by Jonathan Faull, European Commission

Further to the meeting I had with the members of the Home Affairs Sub-Committee of the House of Lords Select Committee on the European Union in Brussels on 28 November, I would like to provide the members with further information regarding the access of UK authorities to the SIS immigration data and the Schengen Evaluation procedure, which were particular points of interest to them. I should be grateful if you would ensure that the position set out below is fully reflected in the record of my evidence.

1. ACCESS BY THE UK TO SIS IMMIGRATION DATA

Following the UK's request, the Council decided in 2000 on the participation of the UK in the Schengen Acquis limited to the aspects linked to police and judicial cooperation in the criminal field.[1] This includes, in particular, access to SIS alerts for arrest and surrender, alerts for discrete checks or specific checks and alerts on persons wanted for a judicial procedure. The limited participation of the UK in the Schengen acquis excludes its participation in the exchange of information via the SIS aimed at the control of external borders or the issuing of visas. As the UK does not participate in these common Schengen policies it has no access to SIS alerts for the purpose of refusing entry.

The recitals of this Council's Decision indicate the following:

> "Whereas it is the view of the Council that any partial participation by the United Kingdom in the Schengen acquis must respect the coherence of the subject areas which constitute the ensemble ofthis acquis;
>
> Whereas the Council thus recognises the right of the United Kingdom to make, in accordance with Article 4 of the Schengen Protocol, a request for partial participation, noting at the same time that it is necessary to consider the impact of such participation of the United Kingdom in the provisions concerning the establishment and operation of the SIS on the interpretation of the other relevant provisions of the Schengen acquis and on its financial implications".

The UK's lack of access to immigration data is also made clear in the draft SIS II legal instruments.

If the UK wants to enlarge its access to SIS data, it should consider participating fully in the Community Acquis related to the creation of an area without internal border controls. The full application of Schengen acquis, which includes access to the SIS immigration data for the control of the external borders or the issuing of visas, would benefit both the EU and the UK. Not only would the UK draw the maximum benefit for UK and other EU citizens as regards free movement, but this would also facilitate the movement of third country nationals travelling into or residing legally in the EU.

2. SCHENGEN EVALUATION PROCEDURE

The Commission has been invited in the Hague Programme "to submit, as soon as the abolition of controls at internal borders has been completed, a proposal to supplement the existing Schengen evaluation mechanism with a supervisory mechanism, ensuring full involvement of Member States experts, and including unannounced inspections".

The Commission has not yet presented such a proposal as the abolition of controls at internal borders with the Member States that joined the European Union in 2004 has not been completed.

15 December 2006

[1] Council Decision 2000/365/EC, OJ L 232/43 of 1.6.2000.

Examination of Witness

Witness: MR DANIEL DREWER, Europol Data Protection Officer, examined.

Q445 ***Chairman:*** Mr Drewer, thank you very much for coming. Particular thanks to you for coming all the way from The Hague. I am sorry you had minor travel problems, but we have had our travel problems too.
Mr Drewer: I believe that you came to Europol in the past, so it is only right that I come to you on this occasion.

Q446 ***Chairman:*** It is very kind of you. We do not want to impose too long on your time. If I may I will go straight into the questions. This meeting is on the record, a transcript will be taken and you will be sent a copy in due course. If there are any points in it that you either want to correct or follow up in writing you are very welcome to do so. Again for the record, this is an inquiry by this Committee into Schengen II. If I could go straight into some Europol questions. What use has Europol made so far of its competence to access and use the data held in the current SIS, and to request supplementary information from Member States? Are statistics available on this? Will statistics on this issue be available regularly?
Mr Drewer: The use by Europol of the Schengen system has not yet taken place because we are waiting for the technical implementation of access. As soon as the practical technical side has been solved there will be statistics on the access that Europol officials will use. The statistics are drawn up by our information management unit, but at the end it is a legal obligation on Europol to keep reports on any retrieval of personal data. There will also be reports on the retrieval of personal data out of the Schengen system. Statistics will be available, yes.

Q447 ***Chairman:*** Thank you very much. Are there plans to increase Europol's use of the current SIS data in practice?
Mr Drewer: Since access to the Schengen data has not yet started it is difficult for me to answer this question. We will have to wait until the technical implementation has been carried out and then Europol officials will have to get accustomed to Schengen data. To my knowledge there are no plans or wishes to extend the use as it is foreseen in the legal provisions.

Q448 ***Chairman:*** I think you have answered my next question which is whether there are current plans to amend or replace the legislation governing Europol's access, and the answer is no.
Mr Drewer: No.

Q449 ***Lord Avebury:*** What effect do you think the SIS II legislation may have upon Europol? Do you think there are any provisions in this legislation that should be more conveniently amended in Europol's view?
Mr Drewer: Since we assume that SIS II will come to Europol in the long-term and access to SIS II will take place at a later stage, a full legal analysis of all the possibilities of SIS II has not yet been made by Europol. We will wait until we get access to the Schengen system as it is now and then we will analyse the situation later on when SIS II is in place. To my knowledge there is no wish from Europol to have more than that foreseen in the SIS II legislation.
Chairman: You may have answered some of Lady Bonham-Carter's next question. Would you like to put it nevertheless?

Q450 ***Baroness Bonham-Carter of Yarnbury:*** I will. What is the process of using SIS data in Europol's operations at present, that is SIS I? In particular, what is the added value of accessing and using SIS data in Europol's analysis work and in its other operations?
Mr Drewer: Europol has to follow specific procedures when it comes to accessing data and other databases. Before we get access to the Schengen system, and the technical implementation is there, we draw up our information flow charts for how the information out of the Schengen system will be handled according to the legal framework at Europol. There are two information flow charts. One refers to the handling of the data that would concern data from third states and international organisations, and one from Member States. The difference is simply that Member States would put their data directly into the Europol systems whereas third states cannot put data directly into the Europol systems, and in this case the information management unit would do it for them in line with the legal provisions. If you ask for a more practical explanation: Europol will check data in the Schengen Information System. If there is an alert Europol will contact the Member State concerned and ask for permission to use the alert information and, if necessary, ask for supplementary information from that Member State, but always in line with the legal provision that says Europol has to obey the restrictions of the Member States given on their information to Europol. The information that Europol will get from the Member State that has been activated by our Schengen alert will be considered by Europol as a Member State contribution to Europol's systems, so it is no longer

Schengen information, it is a Member State's contribution in line with Europol's data protection framework, and from then on we handle it according to Europol's Convention and the applicable secondary legislative framework that we have.

Q451 ***Earl of Caithness:*** I think what you have just said is helpful on this question. Are you satisfied with the rules concerning data protection regarding Europol's access to and the use of SIS data and SIS II in the future?
Mr Drewer: I am Data Protection Officer at Europol and support the Director in ensuring the application of Europol's data protection provisions. From my point of view the data protection provisions foreseen in the Schengen text are pretty much similar to the data protection provisions foreseen in Europol's legislation. To answer your question, you can be satisfied when you have a look at the Schengen Information System data protection rules because effectively they are in line with the rules contained in Europol's Convention. In the Schengen Information System II legislation it is mentioned that Europol should possess the data under its Europol Convention. On the other side, with the Danish protocol to the Europol Convention that will be in place in March 2007, there will be a provision that says when Europol gets data from other systems the legal framework of that international organisation's system should apply to the use of data within Europol. But this does not lead to a conflict in this case because to inform, for example, or to ask for permission to transfer the data to a third party is the same in the Schengen legislative framework as in the Europol data protection framework.

Q452 ***Earl of Caithness:*** Thank you for that. Do you have a record of the number of complaints by individuals or the number of criticisms by the supervisory authorities with regard to how you handle data protection?
Mr Drewer: To answer the first question, there is a record because the complaints that we get are from European citizens, for example, appeals against decisions of Europol to answer Article19 requests. If a European citizen comes to Europol and asks, "You have data stored about me on your database and I would like to be informed about that" and we give an answer to the European citizen, he or she has the possibility of appealing against this. In a sense, it would be a complaint about how Europol's data protection rules affect their daily work. This appeal goes to the Joint Supervisory Body with its currently 25 national data protection authorities that have an eye on how Europol implements its data protection framework. This appeal is then answered by the Joint Supervisory Body. Since we have been operational there have been five appeals against a decision of Europol on how to answer an Article 19 request. Your second question related to criticisms.

Q453 ***Earl of Caithness:*** Criticisms by the protection supervisory authorities of the way you have handled it.
Mr Drewer: Europol has a formalised system on criticism as to how Europol follows data protection rules. This system is formalised in a way that once a year the Joint Supervisory Body visits Europol with a number of national data protection officers. We have an inspection at Europol in all areas of data protection, including the area of information security. Amongst those inspectors who come to Europol there are also IT security experts. Out of the inspection visit there is an inspection report and this inspection report is for the attention of the Director and for the attention of our Management Board. The inspection report includes recommendations to Europol, and you can take recommendations as criticisms in that sense, where the inspectors believe that Europol should have more enhanced data protection measures in place. This criticism in the inspection report, if there is any, is taken up by the Director in the implementation plan of the recommendations which will be checked by the Joint Supervisory Body at the following inspection the next year.

Q454 ***Chairman:*** And would be public?
Mr Drewer: The implementation plan of the Director, who ultimately is responsible for implementing the data protection measures is not public. The inspection report of the JSB is not a public report, it is a classified report, but every two years the JSB publishes an activity report and this activity report is sent to the European Parliament, and this is a public report.

Q455 ***Lord Dubs:*** I understand that under the current rules Europol has a certain amount of immunity. Do these rules prevent Europol from being held sufficiently accountable in respect of its access to and use of SIS data? Will that situation change once the legislation governing the immunity is amended? Finally, how would the situation change again if, as has been suggested, Europol becomes subject to the normal rules on the privileges and immunities of the Community institutions?
Mr Drewer: I think we have to distinguish between the different developments in Europol's legal framework in the future. One is pretty much foreseeable because there will be three protocols that will be implemented next year: the Danish protocol, the protocol on money laundering and the Joint Investigation Team protocol. In the Joint Investigation Team protocol there is an Article which refers to the immunity of Europol staff. This Article

says that as soon as Europol officials are involved in the investigative work of this Joint Investigation Team they are subject to national law, so no immunity is granted to them. I mention this to make clear that it is foreseen that as soon as there are powers given to Europol officials and they become part of this investigation team immunity is automatically withdrawn. If you talk about a Europol official sitting in The Hague at his work station who is data processing in line with Europol's restrictive data protection framework, I do not think a change of this immunity is foreseen, even by the draft Council decision currently under discussion to replace the Europol Convention. I believe there is an Article[1] mentioned that immunity should not change. I am not sure if there are really remarkable differences between the immunity protocol and the protocol for the immunities of the European Communities.

Q456 ***Baroness Henig:*** Do the restrictions on the jurisdiction of the European Court of Justice as regards Europol prevent Europol from being held sufficiently accountable in respect of its access to and use of Schengen data?
Mr Drewer: I believe that the system we have in place now and the restrictions of the European Court stay the same for the handling of Schengen data. The handling of Schengen data within the new legal framework follows the same rules and the same system as applies to any other Europol information. When it comes to judging the activities of a Europol official and the activities of Europol in processing the handling of personal data, then of course our Joint Supervisory Body plays an important role in this with its inspection, its recommendations, its possibility to directly address the Management Board when they deem that Europol has not behaved appropriately regarding the processing of personal data. This is a system that until now has worked efficiently because, apart from the complaints I mentioned before, we have had no case where somebody has asked for jurisdiction over Europol's activities, so we take this as a sign that the system works effectively.

Q457 ***Earl of Listowel:*** The proposed Framework Decision on data protection will not amend the data protection rules in the Europol Convention, but the Framework Decision will apply to SIS II. Will the Framework Decision govern Europol's access to and use of SIS II data or not? What are the practical implications of the answer to that question?
Mr Drewer: Without going too far into a legal analysis of the SIS II text, we would say that the Framework Decision on data protection, even if it applies, will have no practical impact on Europol because what we saw when we did a comparison between the Framework Decision on data protection and Europol's legal framework was that there were not that many differences. Sometimes the Europol data protection framework exceeds the draft Framework Decision on data protection. The answer from Europol's point of view is that Europol's data protection framework will apply to the data that we get first of all through the alert in the Schengen system and, secondly, through the data provided by the Member States as supplementary information. If there should be a check of the handling of information with a view on the Framework Decision on data protection, then the result will be pretty much the same, because the conditions that we have in our legal framework are equal to the ones that are in the Framework Decision on data protection. Of course there are some differences but the differences in our estimation would not affect the Schengen data that will be processed by Europol.
Lord Teverson: In terms of Schengen data being transferred by Europol to other states outside the EU, and presumably you deal with Norway and Iceland anyway and also other non-EU agencies, what is the scope for that under the present and future arrangements? Obviously we have a concern about the onward transmission of data that you would hold.

Q458 ***Chairman:*** Can I just add a supplementary to that and that is, is Interpol at all relevant to that question?
Mr Drewer: When it comes to the exchange of information, and I say Europol information because Schengen information will become Europol information with third states and international organisations, at Europol we need the legal basis for this and we have to follow the provision that is already in the Convention in Article 18 IV, where it says that when Europol would like to exchange Member State's information with a third party it can only be done with the consent of that Member State, that is the owner of the information.

Q459 ***Lord Teverson:*** Can I just ask in a practical sense how that permission is sought? Do you phone someone or email them? Obviously you need a record of some sort of the permission.
Mr Drewer: Any processing of information is recorded according to the data protection rules at Europol. The information can only be exchanged in cases where we have a co-operation agreement with that particular third state or international organisation. We distinguish here between different kinds of agreements. There are operational agreements for the exchange of personal data. There are strategic agreements where it is not allowed to exchange personal data, only so-called strategic information. These are the two types of agreement

[1] Article 50 of the Draft Council Decision.

that we have in place. When it comes to a case where a Member State's information should be exchanged with a third state, we first ask whether an operational agreement is in place. To answer your question, there is an operational agreement in place with Interpol. In this operational agreement there are not just the details in the provisions manifested for the data protection side of the information exchange, you will also find provisions on the confidentiality side and provisions on the IT security side, that is the INFOSEC side, on the exchange of information. The permission to exchange that information with a third state is given by the Member State through a system that we call the handling codes. That means on the particular information there is a handling code and the handling code informs the Europol official what can be done with that information regarding the data protection provisions that are applicable. A Member State could foresee information with a handling code that says "no further dissemination to third states without our consent", so that means the Europol official has to go back to the Member State and ask for written consent that will also be recorded in our system. The handling code says nothing about the confidentiality side of the information because security packages go together with the classification levels that you find additionally on each Europol transmission slip. This tells you, and this is also important for you to know, if there is classified information then it might not be possible to exchange that with a third state, not for data protection reasons, but for confidentiality reasons.

Q460 ***Lord Teverson:*** Are different Member States very different in what they allow? Is there a lot of variability between Germany and Greece, or are they all pretty similar?
Mr Drewer: I am afraid we have not made a study of that but that is an interesting question.

Q461 ***Lord Teverson:*** What is your feeling?
Mr Drewer: I do not have information on that.
Lord Teverson: Thank you.
Lord Avebury: What third countries, institutions and agencies are currently Europol's partners in information sharing? What are the rules and procedures applicable to these exchanges of information? You have partially answered that in your previous answer but in these handling codes are there any which permit unrestricted transfer of data to particular third countries or agencies?

Q462 ***Chairman:*** Can I add to that. What changes would you like to see, if any, to the present rules that govern these exchanges?
Mr Drewer: To answer your first question I can give you the list of our operational agreements. We have operational agreements in place with Bulgaria, Canada, Croatia, Eurojust, Iceland, Interpol, Norway, Romania, Switzerland and the US. Are you also interested in the strategic agreements for the exchange of non-personal data?

Q463 ***Lord Avebury:*** Please.
Mr Drewer: We have strategic agreements with Colombia, the European Commission, the European Central Bank, the European Monitoring Centre of Drugs and Drug Addiction, the European Anti-Fraud Office, with Russia, with Turkey, the United Nations Office on Drugs and Crime and the World Customs Organisation. With the system of the handling codes the Member State can decide and give to Europol any handling instructions, so there is also the possibility for a Member State to use a handling code that is self-defined and, for the empty space on the transmission slip of that operational information, to say that this information should not go to that particular third country in any case or should only go to Iceland, for example. The restrictions of the Member States can be defined. The handling codes system is a flexible system and Europol has to obey any restrictions the Member States give to Europol, although the reason why we have Europol is the exchange of information but in a secure way and under the observation of data protection rules. We have therefore developed a system that respects the handling instructions of the owner of that information.

Q464 ***Chairman:*** Would these rules be affected by your access to SIS data?
Mr Drewer: I do not believe so because the moment we receive the alert and the supplementary information the system that we have in place applies to this area.

Q465 ***Lord Avebury:*** Will the handling codes be attached to the SIS II data?
Mr Drewer: Yes. The moment the Member State provides us with supplementary information, because that information also has to be stored at Europol in one of our systems. It is only possible to store information on our systems when we have a handling code on that information. The same applies if it is information that we get out of the Schengen Information System that is not line in with our mandate. We cannot store it on our systems, and there will be no further dissemination of the information by Europol.

Q466 ***Baroness Bonham-Carter of Yarnbury:*** In limited circumstances, as I understand it, the Director of Europol is permitted to exchange information in the absence of an agreement. That is correct, is it not?
Mr Drewer: Yes.

Q467 ***Baroness Bonham-Carter of Yarnbury:*** How often has he made use of this power?
Mr Drewer: There is the possibility for him to do so as foreseen in one of the Council Acts. There are two conditions foreseen in which he can do this. When he decides to do this he has to inform the Management Board and the Joint Supervisory Body without delay about his assessment. There have been cases in the past where the Director took this right under the Council Act and there has been an exchange of personal data with two third states that are now, in fact, our co-operation partners and who have an agreement. But at that time they had no agreement. Before 2005 there were two cases. Since I became Data Protection Officer in 2005 there have been no such cases and since our new Director, Mr Ratzel, joined Europol in 2005 there have been no cases.

Q468 ***Baroness Bonham-Carter of Yarnbury:*** You mentioned two conditions, what are they?
Mr Drewer: The two conditions are from the Council Act: I believe one is in the essential interest of the Member State and there is a second condition,[2] but I will have to look in the legal text More important is paragraph 4 of the Council Act because it is outlined there that the Director has to inform the Management Board and JSB of his assessment.

Q469 ***Baroness Bonham-Carter of Yarnbury:*** So before he does anything?
Mr Drewer: No. You can imagine that these are decisions taken as a matter of urgency. He takes the decision on the basis of the catalogue that is in the Council Act and later on he has to inform the Management Board without undue delay—that is written in the legal text—that he took the decision and, in addition, he has to inform them of his assessment of the situation when he took the decision to disseminate the data. There were two cases with two of the third states: they are now co-operation partners with operational agreements to exchange personal data.

Q470 ***Earl of Caithness:*** Can I ask you a question which you have not got notice of. There have been a lot of complaints about the quality of the data in SIS I. Have you found difficulty with the quality of the data and has it made your job any more difficult?
Mr Drewer: I believe I cannot answer this question since we have no access to the Schengen Information System. We know about the discussion on the quality of data, which is also a data protection question.

Q471 ***Earl of Caithness:*** Looking forward, is there an input that Europol can make to make certain that the quality of information is what you require to enable you to do your job better so you can direct Member States in that direction?
Mr Drewer: Europol's Director is in the position of having an obligation to look at the quality of the data that we enter into our systems. If the future shows that the data quality is not sufficient then we would have a data protection issue when taking this data into our systems. For this we have a system at Europol called an evaluation code for the information where the sending Member State tells us about the reliability of the information. If you talk about the accuracy of the information, this is something we have to look at as soon as the information comes to us: is the information accurate and can it be processed in our systems. From our point of view these are not Schengen specific questions. These are questions that we have to answer whenever we receive Member States' information.

Q472 ***Chairman:*** One of the points of particular interest to this Committee is the implications of British partial opt-in or partial opt-out of Schengen. Have you got any comments, and by all means go off the record if you prefer, on the implications for Europol of the British partial membership of Schengen?
Mr Drewer: No, I do not. We do not have access yet to the Schengen system. We are not that far, and SIS II will take quite some time. It is not a question that a Data Protection Officer can answer because it is very much connected to the operational side of the business of law enforcement exchange.

Q473 ***Chairman:*** How about your relationship with *sirène* or SIRENE, however we pronounce it?
Mr Drewer: We do not have a direct relationship since we always have to exchange via a European national unit. Our requests for more information go to the European national unit and then they contact the national SIRENE office. That is the way the information is channelled.

Q474 ***Chairman:*** I see. Mr Drewer, we are very grateful to you. Again, I thank you for coming here from The Hague to talk to us. If I may, I would like to thank and congratulate you on the concise and very helpful way in which you have dealt with our questions.
Mr Drewer: Thank you very much.
Chairman: I wish you a safe and happy journey back. Thank you so much.

[2] Council Act of 12 March 1999, adopting the rules governing the transmission of personal date by Europol to third states and third bodies (1999/C 88/01). Article 16 foresees the condition "in the interest of preventing imminent danger associated with crime".

TUESDAY 28 NOVEMBER 2006

Present: Avebury, L; Caithness, E; Dubs, L; Henig, B; Listowel, E; Teverson, L; Wright of Richmond, L (Chairman)

Examination of Witness

Witness: Mrs Laura Yli-Vakkuri, Chair of the Schengen Acquis Working Party, examined.

Q475 ***Chairman:*** Welcome. I think a glass of water is a rather poor response to the excellent hospitality which I enjoyed from your government at COSAC in Helsinki last week. We were very well treated and got rather more than a glass of water.
Mrs Yli-Vakkuri: This is fine for now.

Q476 ***Chairman:*** Mrs Yli-Vakkuri, welcome and thank you very much indeed for coming to give evidence to us. Just for the record, this meeting is on the record. If at any point you want to go off the record you are entirely welcome. In due course you will be sent a transcript of your evidence and you are very free to make corrections and amendments, but if on reading the transcript anything else occurs to you that would be useful to us you are very welcome to send it to us. For the record, again, this is our Committee's scrutiny on Schengen II, SIS Mark II. Thank you for coming to give evidence to us from your very important and crucial position as Chair of the Schengen Acquis Working Party, if I am correct.
Mrs Yli-Vakkuri: Yes.

Q477 ***Chairman:*** Would the Finnish Presidency have preferred the Commission to submit an impact assessment for its SIS proposals?
Mrs Yli-Vakkuri: I was prepared to say something about myself, my Lord Chairman, I do not know if you know who I am.

Q478 ***Chairman:*** I beg your pardon, please do.
Mrs Yli-Vakkuri: Other than I am the Chairman of the Schengen Acquis Working Party.

Q479 ***Chairman:*** I am so sorry, that was very impolite of me.
Mrs Yli-Vakkuri: No, no. Just for the record, I come from the Ministry of the Interior of Finland, the Unit for International Security Affairs. This time around—this is the second Finnish Presidency—I have chaired two working groups, the Schengen Acquis and the Schengen Evaluation Working Party which deals with Schengen enlargement issues. The last time around in 1999 I also chaired the Schengen Acquis Working Group. As to the SIS II legal instruments, I am a lawyer so I can say that as a lawyer it was indeed a privilege to be involved in this negotiation process within the Council and the European Parliament because we are talking about an important information system. Even on a global scale it is a huge system. Now we have reached political agreement on this issue and we are waiting for the formal entry into force of these instruments because the linguist lawyer process still takes a few weeks, if not more, and there are still some parliamentary reservations pending concerning in particular the third pillar instrument in this package. You went straight to the first question of the questions that were sent to me. Yes, normally, ideally, of course, legislative instruments should be accompanied by an impact assessment. That would be preferable in normal cases. In this case it was not that necessary because it had been decided already in 2001, if I remember correctly, that there was a need to develop a second generation Schengen Information System. The decision had been taken then by the Council so it was for the Commission to implement that decision. The Schengen Information System has been in use for ten years now so the Member States know how it works. These SIS II proposals did not change the fundamental issues in that system, we are just developing them further. Ideally, yes, but maybe it was not absolutely necessary in this case.

Q480 ***Chairman:*** No, right. Perhaps I could ask an unscripted question because we have heard quite a bit today from other witnesses about a Portuguese proposal for an SISone4all. Would you like to give us your reaction? How does this affect your Working Party's work? What impact is it going to have on progress, or lack of progress, of SIS II?
Mrs Yli-Vakkuri: Indeed, Portugal presented this proposal to the Council in September/October in order to facilitate or speed up the process of Schengen enlargement vis-à-vis the new Member States. During this autumn the relevant working groups have been discussing the proposal, the technical feasibility, the legal, technical, operational and management issues related to this proposal. In fact, at this very moment some conclusions are being drafted in the Justus Lipsius building concerning the outcome of this study and these conclusions will be presented to the Council next week on Tuesday. We

know already that in principle this solution could be technically feasible but the effect on the SIS II project as far as technical issues are concerned is still under discussion.

Q481 ***Chairman:*** Is it likely to further delay the process, do you think?
Mrs Yli-Vakkuri: There is always a risk because you can take a political decision saying that one or other of the options is the priority but we are the same people working with these projects and we are only so many. Obviously one cannot exclude that these projects affect each other's timetables. We could be talking about a few months maybe, I do not know. We will need to discuss that between the ministers on Tuesday.

Q482 ***Chairman:*** Thank you. Does the Presidency believe that the process of negotiating the SIS II legislation was transparent enough for the public and for national parliaments? Does the Presidency have any plan to address the transparency of the co-decision process, in particular the informal discussion between the European Parliament and the Council and the process of reaching "first reading" agreements?
Mrs Yli-Vakkuri: This is a good question because we are talking about legal instruments which will come into force and be directly binding on Member States and citizens, so obviously transparency is important. Also transparency issues are close to the heart of the Finnish Presidency as one of our priorities.

Q483 ***Chairman:*** Indeed.
Mrs Yli-Vakkuri: I would say that the rules on transparency within the Council have developed a great deal during the past years. Concerning legal instruments, like here in the context of the SIS II, the working documents have been made public if there has been a request to the Council to do so. Throughout the process all the working documents, revised versions of the original Commission proposals, have been distributed if such a request was made. That is as far as the documents are concerned. As far as the negotiations or deliberations within the institutions are concerned, when these issues have been discussed in the Council there is always a press conference afterwards and the conclusions are made public, so in that sense the public and national parliaments are able to follow the process. As far as the working level discussions are concerned, let us say that as to the working groups within the Council or the informal meetings with the European Parliament, it would be quite difficult to make them public. But the results of these discussions are always based on and will be reflected in the documents that are made public if such a request is made.

Q484 ***Earl of Caithness:*** I have a supplementary that is on the transparency of the existing system. When the French ran the Schengen office a lot more information was produced before 1999 when it became part of the EU, and it was only recently due to a public outcry that more information was released about how the present system is working. Why do you think that happened, that there was a sudden reduction in the amount of statistics and information available in 1999? What have you been doing to satisfy the demand for a clearer and more transparent system?
Mrs Yli-Vakkuri: That is an interesting question. I did not realise that was the case.

Q485 ***Earl of Caithness:*** Would you like to write to us about it?
Mrs Yli-Vakkuri: I am sorry I am not able to reply, I did not know that there was such a decrease in transparency after 1999. I am sure that was not the intention when we integrated the Schengen Information System and the whole Schengen system into the European Union. As I said, the transparency rules are developing and with the SIS II we will see even more transparency and more involvement by the European Data Protection Authority, for instance, so let us hope that things will get better then.

Q486 ***Lord Avebury:*** My question is about the various negotiations between the Parliament and the Council and whether you can identify significant parts of the texts which can be attributed primarily to the Parliament in the face of the Council's reluctance to accept them and, conversely, whether you can also identify the provisions which are primarily the work of the Council in spite of the Parliament's reluctance. Can I ask you to illustrate that by reference to a document which was presented to the Parliament on 23 October and which we understood was approved by them on that occasion which has now gone to Council where we are told there is substantial agreement and it may just go through on the nod with one minor exception to do with a matter that has been raised by the Germans concerning their security force's access to certain information. Is the process really one of substantial agreement or can you identify places in which there has been controversy and where the final text represents the best compromise that could be achieved between the Parliament and the Council?
Mrs Yli-Vakkuri: Yes. First of all, may I just clarify or emphasise that in October a political agreement between the institutions was reached so we will not touch the text itself any more. We are not negotiating the provisions any more. The only slight changes that we might still have to see in the text will be the results of the linguist lawyer process. You spoke about reluctance, I think that is quite a strong word because

here we are speaking about the negotiation process, we are speaking about co-decision, we decide together. When two institutions discuss we first have a basic text and then we discuss amendments. We present the proposal and we have to present and justify the amendments in a convincing way. In the end, and I think this was confirmed throughout the negotiations, all the institutions were working towards the same goal. The SIS II should be a secure system, it should be a safe system, it should be an efficient tool for law enforcement authorities and, very importantly, it should guarantee some basic rights for individuals. We are all working towards the same goal, but maybe the Member States are more experienced in knowing how the system operates so when there is a proposal, let us say from the European Parliament in this case, and the Council discusses it, and because we are all sensible people we accept the idea if it is found useful but we have to look at the drafting to ensure it works in practice. I would not say that there was a reluctance towards Parliament's proposals but every proposal was discussed and justified as to why it could or not could be accepted, and if it could be accepted in most of the cases we did some drafting, again together with the European Parliament. You asked also who could be the mother or father of certain provisions in these documents. I would say that the European Parliament contributed a great deal to the provisions that concern the security of the system, for instance, and to the data protection rules as well. Parliament was very strong on those points and concerning the provisions which ensure that the central system and the national systems function together in an efficient and safe manner.

Q487 ***Chairman:*** Thank you very much, that is very helpful. Obviously this Committee is interested in the whole range of questions but perhaps most particularly in the role of the British Government and their representatives in Brussels and, with permission, a representative is sitting behind. Could you tell us either on or off the record your reaction to the role that the British machine has taken given the fact that we will not participate in the adoption of the regulation governing SIS II immigration data. How much impact does the British input have given this rather curious situation we are in of being only partially in Schengen? If you want to go off the record you are very welcome.
Mrs Yli-Vakkuri: As we go along I will indicate if that is necessary. First of all, I mentioned that I am a lawyer, if I can still say that after 17 years of government service. For a lawyer the Schengen world is a fascinating world, or justice and home affairs in general in fact, we have so many exceptions, opt-in, opt-out, it is quite interesting sometimes. As far as the negotiation process on the SIS II legal instruments is concerned, we started discussing these instruments during the UK Presidency so the UK had a big impact in the beginning because they had a privileged task but also a difficult task in managing the first reading of those documents in the Council. As already has been discussed, this is a huge and important system so obviously the discussions at the beginning were quite difficult in the sense that people did have views, but maybe people did not understand all the provisions included in the Commission proposals, and under the UK lead we had to go through all those provisions. I am not convinced that the fact that the UK does not participate in all parts of the Schengen Acquis affected the discussions on these instruments that much. If you have a look at these two basic instruments—of course there are three instruments—the decision and the main regulation, many of the provisions are horizontal as far as the establishment of the system is concerned. The functioning of the system, the processing of data, et cetera, et cetera, all of these are horizontal provisions. The UK participated fully in the adoption of these parts in the context of the decision. This is what I can say from the process, the UK participated as a normal Member State in the discussions.

Q488 ***Earl of Caithness:*** My question is almost a supplementary to what the Chairman has just asked. In particular you reminded us that all this discussion started during the UK Presidency. Did our position affect our ability to chair the meetings either positively or negatively?
Mrs Yli-Vakkuri: I do not think it did that much, probably not, no. In any case it was difficult. When you do a first reading of a huge legislative package like this it is in any case quite difficult, so I would not say so.

Q489 ***Lord Dubs:*** What concerns have Member States expressed about the Commission's record of managing the SIS II project to date? I am aware it is a very complicated project indeed. Is the Presidency happy that an agency will be created to manage SIS II following management by Member States for an initial period?
Mrs Yli-Vakkuri: First of all, on the managing of the SIS II projects, there have been some drawbacks. For instance, the process of call for tenders, for instance, was not that successful and the Commission had to go to court even which caused some delays to the process. This was a concern. If we think of the SIS II as a whole it is a common project, it is not just the Commission who manages it, it is also the Member States who implement it and they have national systems which they will have to update. It is not only the Commission who has to deliver here. Throughout the process it has been indicated that all these, can we

call them stakeholders, need to deliver. Of course we are speaking about a system which started as a system developed between the Member States and managed by the Member States, so obviously it is a question of building trust as well between different parties. As far as the future is concerned, the Finnish Presidency is quite happy with the solution that was found in these legal instruments. We foresee the establishment of a management authority. This management authority should be an independent agency who would then manage the SIS II. We think that it would have delayed the adoption of these instruments had we tried to develop or decide on this agency this year, so it is quite good that we have an extra two or three years before we have to establish that agency. Our view is that it should be an independent agency.

Q490 ***Lord Avebury:*** You said just now that the call for tenders was not successful. Do you attribute that to a management failure of those who were drafting the tender documents or was it simply that the people tendering were not the right organisations to undertake this particular project?
Mrs Yli-Vakkuri: I am afraid I cannot answer that question because I am not an expert on the technical side. I am sorry, I am not very familiar with that process.

Q491 ***Lord Avebury:*** You made the remark in the context of Lord Dubs' question about the Commission's record of managing the project.
Mrs Yli-Vakkuri: Yes.

Q492 ***Lord Avebury:*** I take it that in fact this was, indirectly at least, a criticism of the manner in which the Commission handled the tendering process.
Mrs Yli-Vakkuri: I mentioned some of the problems that the Commission was facing.

Q493 ***Baroness Henig:*** Part of my question has already been answered. You obviously expressed a preference for an independent management agency.
Mrs Yli-Vakkuri: Yes.

Q494 ***Baroness Henig:*** I just wondered whether the Presidency would support management of the Schengen II by Europol or by Frontex and what your views on that would be.
Mrs Yli-Vakkuri: Indeed our preference would be for an independent agency. We did discuss the two options you mentioned in Helsinki and they have been discussed between the Member States as well, or at least we had a preliminary discussion in spring. In Helsinki, the way we see it is that Europol is not an EU agency, at least it is not yet, so we see that as a problem because if you create an EU agency then this agency would function under the EU rules directly. Furthermore, Europol is a third pillar agency in a way, or will probably be a third pillar agency concentrating on law enforcement cooperation, while SIS II is an inter-pillar system which deals on the one hand with border control management issues and, on the other hand, it is a law enforcement tool for police organisations. Europol is not designed for doing this kind of work. The same goes for Frontex. Frontex is a border management agency. We are also talking about an important police co-operation aspect here.

Q495 ***Chairman:*** I am sure I do not need to tell you that the United Kingdom is by no means the only country in the European Union which has had some very unhappy experiences with large IT projects. Are you convinced that there is somebody or some organisation out there actually competent to take on this enormous project?
Mrs Yli-Vakkuri: Well, we certainly hope so.

Q496 ***Chairman:*** So do I!
Mrs Yli-Vakkuri: Obviously we will wait for the Commission proposal on this but we have tried to make the Commission's work a little bit easier because in these instruments we have developed rules on how to manage this system. There are quite a few clear rules related to security, exchange of information, et cetera, et cetera. We are not talking about easy things. There are other large scale IT systems being developed at the same time, so at some point we will need to discuss the interoperability of these systems.

Q497 ***Lord Dubs:*** Have you got any that work?
Mrs Yli-Vakkuri: The Schengen Information System works very well at the moment.
Lord Dubs: But it is smaller.

Q498 ***Lord Avebury:*** In any case, by the time it gets handed over to the agency the design and development work will already have been accomplished, will it not?
Mrs Yli-Vakkuri: Yes.

Q499 ***Lord Avebury:*** For whoever is appointed to conduct this phase of the development it will become clear by the time the agency is appointed whether it is working or not and it will be handed over as a working system, I presume.
Mrs Yli-Vakkuri: Yes.

Q500 ***Earl of Listowel:*** Mrs Yli-Vakkuri, continuing our discussion of this agency, may I ask you whether the Presidency has a view about what mechanisms should be adopted to ensure the accountability of this institution?

Mrs Yli-Vakkuri: As I mentioned before, in these instruments we do already have quite a few rules on this. We have defined the basic responsibilities which this authority should take. We have rules on security, confidentiality, keeping of records, the processing of data, et cetera. The basic rules are already there. I am sure that when we do discuss that Commission proposal in the coming years we will have to see whether there is something we need to change in these basic instruments to ensure accountability.

Q501 ***Earl of Listowel:*** So there will be an annual report and any shortcomings would be addressed in that report?
Mrs Yli-Vakkuri: Yes, I would imagine so, because this system will probably start functioning before we have that agency, so we can gain experience and then we will see. We do have quite convincing data protection rules in these instruments. We have the national data protection authorities who supervise the system from the national point of view, we have involved the European Data Protection Authority and we have rules on how to link the work at national levels and European level so that these data protection authorities can discuss and address issues of common interest.

Q502 ***Lord Teverson:*** I would like to ask what view the Presidency takes in terms of the delays in implementation of SIS II and I suppose very directly who is responsible for those delays? Perhaps I can leave it at that and you can talk us through that.
Mrs Yli-Vakkuri: Yes, the blame game. As I said earlier, this is a common project and we have done quite a lot of research work on the development of the system and we have had to adapt the timetable of this system as we have gone on with the process and, indeed, there are still some unknown factors. We do not know if we will accept the SISone4all solution, for instance. It is a common project and I think it is safe to say that nobody is perfect. You can always blame the Commission and say that they could be more efficient or there is a lack of experience or something like that. This can be said but, of course, there have been some reported delays at the national level as well and at the central level. We need to understand that this is a common project and we are trying to manage this project in a way that all the interests are met. In fact, the Council has established an SIS Task Force to oversee the technical development.

Q503 ***Lord Teverson:*** Just to take that slightly more broadly. Although there have been delays if, say, SIS II was ready next week, because this is just the technical systems side, are the potential new members of Schengen ready? How ready would you judge them to be in terms of the evaluation side that has to take place? Is your feeling that on the whole if the systems were ready it could be practically implemented on the ground or is there still a long, long way to go in terms of secure borders and that sort of side in terms of the East European states?
Mrs Yli-Vakkuri: Not that long. If we are talking about next week, no, they would not be ready next week. In fact, the Council next week will discuss the Schengen implementation in the new Member States and we are going to discuss the progress report prepared by the Presidency concerning the ability of these new Member States to implement Schengen rules. When we talk about Schengen implementation it not just that you change laws, you may have to change operational structures, you need to have sufficient infrastructure at the air borders, land borders, sea borders, et cetera, so this process takes time. We need to have target dates. The target dates we have been speaking of so far are somewhere towards the end of 2007. I would say that no new Member State will be ready tomorrow or even early next week because we need to give national administrations some leeway there to organise themselves. At some point before that target date we need to decide whether we are convinced that these new Member States are able to apply the Schengen Acquis in full. The progress report concerning the evaluations that took place in 2006 are quite positive in the sense that a lot of progress has been made but some infrastructural changes or adaptations still need to be done and even some laws still need to be changed. The process is going along very well, I would say.

Q504 ***Lord Teverson:*** Thank you very much.
Mrs Yli-Vakkuri: There will be a report next week to the Council. We are preparing the conclusions on this.

Q505 ***Earl of Caithness:*** Can I turn Lord Teverson's question round for you. Given that since the late 1990s we knew that there was going to be an expansion of the Member States and that Schengen would have to be improved and enlarged, and here we are eight years later still floundering, what are the lessons to be learned for the Commission, the Council and the Member States in all of this? Surely we have got to find something so that some of the horrendous mistakes that have been made do not happen again. Is that something that you and the Presidency are addressing?
Mrs Yli-Vakkuri: First of all, I am not sure that there have been huge mistakes because if you look at the history of Schengen, Schengen has always been enlarged in steps. If we start from the beginning, the Schengen Convention was signed in 1990, it entered into force in 1993 and the full implementation started in 1995. Even the original Member States needed five

years to prepare for that. For the Nordic countries, and we are good pupils, it took four or five years as well. We signed the Schengen Accession Agreement in December 1996 and started applying the Schengen Acquis in March 2001. For some other Member States it has taken up to seven or eight years to start implementing Schengen. It has always been a two-step process. First of all you express the will to be part of Schengen and then the process starts and it takes X years. The new Member States acceded to the European Union only two years ago so I think we have worked quite fast, although it is true that we started already before accession working with them with this ultimate goal—the full Schengen implementation—in mind. We have prepared for this decision for some years. I would not speak about crucial mistakes in this context.

Q506 ***Lord Avebury:*** Has the Finnish Presidency got any view about whether or not, and in what circumstances, the UK should participate in alerts for the non-admission of third country nationals? If you as a lawyer could imagine that there are perceived advantages, not only for the UK but for all other European states in having such a system which would enable more effective management of the immigration process throughout the whole of Europe, have you any views on how that access should be organised legally and in practice?
Mrs Yli-Vakkuri: If we start with the legal basis for all this. There are the rules in the UK protocol to the Treaty of Amsterdam, there is a Schengen protocol to that same Treaty, and in accordance with those rules the UK applied for a partial application of the Schengen rules and this UK application was dealt with in 1999 and the final decision on the UK application was taken in 2000. In that application, and indeed the Council finally was in favour of the UK application, and in that decision the UK does not participate in the provisions of the Schengen Acquis which deal with border control issues or the refusals of entry. This is quite clear. This is the legal basis. The UK did not apply for participation in the provisions related to the entry to the Schengen area.

Q507 ***Lord Avebury:*** That is *res judicata*, you cannot imagine any revision of that.
Mrs Yli-Vakkuri: Unless we received an application from the UK to participate in these provisions and then we would deal with the application in accordance with the Treaties. As far as the Schengen Information System is concerned, and as a result of that basic decision on the UK Schengen application, a filter is foreseen in the Schengen Information System so that alerts on refusals of entry will not be used in the UK. This is a result from that basic decision that the UK does not apply these rules. Of course you can always ask why will we not give access to the asylum authorities, they are not guarding the borders, they are dealing with these issues from a different perspective, but then you have to bear in mind that we are talking about the Schengen area and the purpose of the alerts on refusals of entry is to refuse entry to the Schengen area, so the reason why the Schengen asylum authorities of some Schengen states have access to these alerts is quite logical, but that would not be the case for the UK asylum authorities.

Q508 ***Chairman:*** It is quite clear that the UK position on this partial opt-in or partial opt-out has disadvantages for the United Kingdom, you have made that very clear. Can you just speculate a little what disadvantages does it have for the other members?
Mrs Yli-Vakkuri: The Schengen system is—I can speak from five years experience of being a member of Schengen—quite an important law enforcement tool for Member States, so it is quite regrettable that not all EU Members can fully participate in this system. I would say for law enforcement purposes it would be nice to have everybody in.

Q509 ***Chairman:*** For both sides?
Mrs Yli-Vakkuri: Yes. It is about exchanging information.

Q510 ***Chairman:*** Presumably the Commission are even now working on proposals for harmonising alerts, for non-admission of third country nationals, rules on flagging, certain criminal law and policing alerts, and rules on remedies in the context of data protection. Is the Presidency actively involved with the Commission in drawing up these proposals?
Mrs Yli-Vakkuri: Given that it was only a few weeks ago that we finalised this text I am not sure how far the Commission is in its thinking. I would say that during the Finnish Presidency nothing will happen. We are feeling relieved that we have finalised this package. As far as the Commission proposals you have mentioned are concerned, they were seen to be quite important in the sense that many Member States feel we need to have a look at these rules after the system has been functioning for a few years. We are looking forward to dealing with those proposals, but not during the Finnish Presidency!

Q511 ***Earl of Caithness:*** I would like to take a slightly wider view now and make the question a bit broader. What are your views about the interoperability of EU databases?
Mrs Yli-Vakkuri: It is an interesting question and worth exploring, I would say. We have received, and you have probably seen it as well, a Commission communication on this subject which was submitted a year or so ago. The Council has not had the

possibility yet to discuss the ideas in the Commission proposal in detail. We have addressed the issues but as we have been developing these systems we have not started in-depth discussion about interoperability. Of course, some basic issues need to be discussed. First of all, we need to see if it is technically possible. Secondly, we need to ensure that important basic rules of data protection, for instance, will be respected. From the technical point of view there has already been a discussion that the VIS system and SIS system would have a common platform, for instance, so from the technical point of view things have developed towards that goal. From the legal point of view we need to have a look at this question on the basis of the Commission's communication.

Q512 ***Lord Dubs:*** Can the Presidency make available any information or statistics about the practical operation of SIS II in Finland?
Mrs Yli-Vakkuri: Yes, indeed it can. I have those statistics with me but they are in Finnish so I decided to ask my colleagues to send them to me in English. I was not precise enough when I asked for those statistics. If I may, I could send them separately.

Q513 ***Chairman:*** Would you be prepared to send them to us?
Mrs Yli-Vakkuri: Sure, yes.

Q514 ***Chairman:*** It would be very helpful if you would.
Mrs Yli-Vakkuri: We have been in operation now for five years. I do not know whether you would like to have an overview of everything.

Q515 ***Chairman:*** I think it would be very helpful to have a sort of mood view from you.
Mrs Yli-Vakkuri: I could provide some information in writing.

Q516 ***Chairman:*** If you have anything you want to say now about how the SIS system is working in Finland that would be helpful.
Mrs Yli-Vakkuri: Just today, because we are discussing SIS issues every day right now, and it is the pre-Council time and the Council next week will be an important Council from the Schengen and SIS point of view, I discussed this with the head of the Finnish SIRENE office and we discussed the Finnish experiences and she confirmed that the Finnish law enforcement authorities are very happy to be part of Schengen, it has made international co-operation much easier and much more efficient. Now we have a means of exchanging law enforcement data this with each other in an efficient manner, even in structured form. SIS includes a system of exchanging forms, for instance, so it is very easy to see what the information is about. I am not a technical expert but I know what these forms look like.

Q517 ***Chairman:*** Before your entry into the European Union there was presumably quite a lot of exchange with your Nordic neighbours at least on immigration, asylum and crime?
Mrs Yli-Vakkuri: Yes. We felt that it was quite important that all five Nordic countries entered Schengen at the same time. We saw that as essential.

Q518 ***Chairman:*** Is your co-operation with Norway affected by the fact that Norway is not a member of the European Union?
Mrs Yli-Vakkuri: Yes, it is. As you know, the Council has an agreement with Norway, Iceland and Switzerland concerning Schengen issues and they participate in the Council meetings.

Q519 ***Chairman:*** As if they were members?
Mrs Yli-Vakkuri: Let us put it this way, they cannot take decisions. They can participate in the discussions, they can bring forward proposals and say if they have a problem with a certain proposal but when the formal decision is taken, when we count the votes, they are not in that count.

Q520 ***Chairman:*** I think my last question is from your point of view how do you see the readiness of new members, particularly Bulgaria and Romania, at this point in time to take part in these discussions and these proposals?
Mrs Yli-Vakkuri: Bulgaria and Romania, as from the signing of their Accession Agreements, have participated in the Council work as observers, so they have had the opportunity to follow the discussions as far as Schengen enlargement issues are concerned and I think it has been a very useful and helpful opportunity for them to learn as well, so we hope that after 1 January they can start participating more actively.

Q521 ***Chairman:*** Be fully involved?
Mrs Yli-Vakkuri: Yes.

Q522 ***Lord Dubs:*** I wonder if I could just follow up on this wider issue. You mentioned that there were a number of countries within Schengen that were not in the EU, and you mentioned Norway, Iceland and Switzerland, and then you have got Denmark, Britain and Ireland who are in the EU but not in Schengen.
Mrs Yli-Vakkuri: That is why I said that Schengen is a paradise for lawyers.
Lord Teverson: Denmark is in Schengen.

Q523 ***Lord Dubs:*** Denmark is not in Schengen.
Mrs Yli-Vakkuri: It is in Schengen but it has an opt-out concerning other first pillar matters in the EU.

Q524 ***Lord Dubs:*** Leaving aside the work that this produces for lawyers, I take it there is no thought given to other countries being able to be part of Schengen who are not in the EU on the model of Switzerland, Norway and so on? Are we saying Schengen is there and the only extension will be if other countries join the EU?
Mrs Yli-Vakkuri: I would say that geography plays a big role here. By the way, we are negotiating with Liechtenstein at the moment. I have not heard of any other further applications.

Q525 ***Lord Avebury:*** How about Kaliningrad?
Mrs Yli-Vakkuri: Kaliningrad, yes.

Q526 ***Chairman:*** An interesting question.
Mrs Yli-Vakkuri: An interesting question.

Q527 ***Chairman:*** You need a few more lawyers for that.
Mrs Yli-Vakkuri: Indeed.

Q528 ***Lord Dubs:*** Would you mind if I went back to the point you answered a little while ago about the British position as regards sharing information on immigration.
Mrs Yli-Vakkuri: Yes.

Q529 ***Lord Dubs:*** You said from the point of view of law enforcement it would be a good thing if this information were shared.
Mrs Yli-Vakkuri: Yes.

Q530 ***Lord Dubs:*** Are you reflecting a unique position in this or is there a wider view that, in fact, the countries that are not in Schengen could usefully exchange immigration information with Schengen in order to help with law enforcement? It is a point that our Chairman made a little while ago. Is there a sense that there might be some movement on this? You have made a more positive statement than perhaps some people have.
Mrs Yli-Vakkuri: These matters are being discussed all the time. Let us say it is a horizontal issue in a sense because we are talking about fighting organised crime and terrorism and so on, so in the context of these discussions these points pop up. I do not know, I am not an expert on police co-operation so it would be difficult for me to answer. If we go back to the data on refusals of entry, for instance, even though the UK does not have at the moment, or will not have, direct access to these alerts, the EU instruments dealing with asylum issues—the first pillar instruments in which the UK does participate and which are not Schengen related—provide for co-operation between the Member State authorities so the UK has the possibility to discuss this with colleagues from other countries on the basis of those instruments.
Lord Dubs: I think you are right about how good it is for lawyers!

Q531 ***Lord Teverson:*** I had not realised Switzerland was part of this system actually.
Mrs Yli-Vakkuri: Not yet. The agreement with Switzerland has not entered into force yet, there are still some parliamentary reservations left. They will enter into force quite soon I would expect.

Q532 ***Lord Teverson:*** In terms of the civil liberties or the control aspects related to Schengen and the use of the information, does that mean that the regulations effectively have to be passed by those national parliaments more or less as they are in the EU? That is presumably a condition and they are pretty well identical to the equivalent EU regulations in terms of data protection and that sort of stuff.
Mrs Yli-Vakkuri: There is a guillotine clause, I do not know if you can call it that. If the associated states—Iceland, Norway, Switzerland—refuse to adopt or apply a Schengen related legal instrument the Council will have to determine what to think of that and then in a very hypothetical case the third country concerned would be left outside Schengen. This is really hypothetical, it has not happened yet and it would be very difficult to foresee this kind of situation.

Q533 ***Lord Teverson:*** For Norway and Iceland and Liechtenstein it is similar to the EEA procedures anyway in terms of reflecting Directives and Regulations?
Mrs Yli-Vakkuri: Yes.

Q534 ***Lord Teverson:*** But Switzerland is obviously different.
Mrs Yli-Vakkuri: No, it is not different. The rules are the same for them as for Norway and Iceland. Switzerland does not apply Schengen yet. After their agreement has come into force the normal Schengen evaluation process will start and it will take some time, so we are not talking about something which will happen even next year, we are probably talking about 2008 at the earliest.

Q535 ***Lord Teverson:*** Do they pay part of the developments costs of the SIS II system?
Mrs Yli-Vakkuri: Yes.

Q536 ***Earl of Listowel:*** You mentioned that you are involved with Schengen evaluation as well. Can you say a bit more about the Schengen Evaluation Team

and in particular perhaps about possible developments of it, for instance no warning visits or how co-operation with authorities in the monitoring process might be improved. What about pressures to go forward once the assessment has been made even if there are questions within the assessment provided by the evaluation team, the political pressures to go ahead? Are you calm about that? Do you feel any concern about that? Finally, can you indicate what sort of worst case scenarios you have thought of in terms of the abuse of the data provided either by an individual or perhaps leakage to organised crime? Perhaps that is a bit far from your experience.

Mrs Yli-Vakkuri: I have been involved in the Schengen evaluation work since 1998 or 1999 and I have followed the evaluations of the Nordic countries and the recent evaluation processes. The Schengen evaluation consists of two parts. First of all you have the evaluation of the possible newcomers, and that is what we are talking about in respect of the new Member States now, and then you have an ongoing evaluation of the Schengen states who already apply Schengen. The Schengen system is based on trust, so you have to trust the others and from time to time you want to check that everything is okay in the other Schengen states. That is the other aspect of the Schengen evaluation. We do have a working group, which is called the Schengen Evaluation Working Party, which meets here in the Council. I am the Chairman of that working group during the Finnish Presidency. We are horizontalists obviously, nobody can be an expert on all issues. This Working Party has established evaluation committees for all aspects of Schengen—including the land borders, air borders, sea borders, police co-operation, visas, data protection—and these committees visit the countries concerned. For instance, this year has been quite heavy for the experts because we have had to visit ten Member States and we have had six subject areas. Normally you do not visit a country for half a day or one day only, you spend some time there, you travel along the border, et cetera. We did 58 evaluation emissions this year, we assessed and discussed the reports in this working group and now we are finalising the conclusions. Concerning the information that is received and discussed during the evaluation process, until now they have been so-called restricted documents so it is understood that this information is confidential by nature.

Q537 ***Earl of Listowel:*** That is very helpful, thank you. Are you concerned that having done all this work political pressures will perhaps push things forward when the careful reports you have made do indicate some concern about a particular area in a particular country? When I was talking about the sensitivity of the information and the worst case scenarios I was thinking of if a country was not doing a good enough job at safeguarding this information what is the worst case scenario from the point of view of a data subject that you could imagine happening to that person? What is the worst case scenario in terms of organised crime or whatever else obtaining access to the Schengen system, being able to know when an alert is going out about somebody being surveyed or something like that? Perhaps that is a bit far away from your experience. What you have said so far has been very helpful and perhaps that is as much as is necessary for you to say at the moment.

Mrs Yli-Vakkuri: Again, I must say that nobody is perfect, not even Finland, although we were assessed quite positively concerning our borders. At some point you will have to decide that the trust is there and the Schengen Acquis is implemented in a satisfactory manner. This assessment may include, for instance the verification of whether a stamp is placed in the right place on the passport. As you can see, technical issues like that are assessed and but obviously more crucial issues are emphasised. This is where the evaluation process truly comes into play. You may have to visit these countries again and see whether the weakness has been remedied or not. It is an ongoing evaluation. It is in The Hague programme, by the way, that the Commission will submit, I think next year, a proposal to develop the evaluation procedures in the justice and home affairs areas so we will debate and see how we should develop the system.

Earl of Listowel: Thank you very much.

Q538 ***Chairman:*** Mrs Yli-Vakkuri, thank you very much indeed. You have given us very helpful answers to our questions, we are most grateful to you for coming. We wish you good luck in the remaining 31 days of your Presidency.

Mrs Yli-Vakkuri: Thank you very much. It is true that we are counting the days!

Q539 ***Chairman:*** But you are taking a few days off for Christmas, I hope?

Mrs Yli-Vakkuri: Yes.

Chairman: Thank you so much.

WEDNESDAY 29 NOVEMBER 2006

Present	Avebury, L	Harrison, L
	Caithness, E	Henig, B
	Corbett of Castle Vale, L	Listowel, E
	D'Souza, B	Marlesford, L
	Dubs, L	Teverson, L
	Foulkes of Cumnock, L	Wright of Richmond, L (Chairman)

Memorandum by Joan Ryan, MP, Parliamentary Under-Secretary of State for nationality, citizenship and immigration, the Home Office

The Operational Management of SIS II by the Commission, and Whether the Rules Ensure Accountability

During discussions on SIS II, the provisions on management of the system have been extensively discussed, in order to ensure that the system continues to function effectively during the transition from SIS I+ to SIS II, while being established on a firm legal base.

As a result, the provisions relating to management have been amended, allowing for a short- and long-term solution to the management of SIS II. In the short term, the Commission will be responsible for management of SIS II. In practice, it will delegate this responsibility to the authorities in the Member States where the existing system, SIS I+, is located (France and Austria). There are clear rules on how responsibility will be delegated, and the duties and obligations on the Commission and the authorities to which management is delegated.

In the long term, it is unlikely that the Commission will be given responsibility for the operational management of SIS II. Several options have been proposed for the long-term solution for management of SIS II. These include management by Frontex (the European borders agency), Europol, the Commission, or a new cross-pillar agency. Of these the first two have been rejected. The UK does not participate in Frontex (which is purely first pillar), and Europol is a third pillar body funded by the Member States rather than the Community budget, so neither is ideally suited to hosting a database holding both first and third pillar data. Management by the Commission proved unpopular with most Member States.

Most Member States support the creation of a new cross-pillar agency to manage SIS II, subject to a suitable impact assessment. The legal instruments therefore provide for a Management Authority to be responsible for the long term operational management of SIS II. The advantage of a cross-pillar agency is that it would reflect the first-pillar immigration content of SIS II, as well as the third pillar law enforcement content. The Government believes that this option provides the most sensible solution to management of SIS II in the long term, and will ensure that the Commission conducts a full impact assessment and considers, among other things, whether or not SIS II should be co-located with any other EU database. The legal instrument contains strict rules on security and confidentiality and record keeping that must be complied with by the Management Authority.

The Implications of Including Biometric Data

The addition of biometric data into the SIS II will provide significant improvements to the accuracy of the system making misidentification less likely. The insertion and use of biometric data will be subject to strict controls. Searching using biometric data will not be permitted until the necessary technology is available, which will ensure that misidentification of persons is minimised. Additionally, where there is a possibility that confusion may arise between the subject of a SIS II alert and another person, adding biometric data will greatly aid the prevention of the negative consequences arising from misidentification, as it will be possible to quickly establish where an individual is not the same person against whom an alert has been issued. The Government believes that there are strict safeguards in place to ensure that the addition of biometric data into SIS II will not compromise data protection.

The Provisions on Allowing Interlinking of Alerts

Allowing alerts to be linked will improve the functioning of the system. Links between alerts will not be allowed unless there is clear operational need for a link to be made. The Government believes that linking alerts will help with the aim of SIS II, ie the prevention, detection and investigation of crime. For example, the details of a stolen car in which it is believed an abducted child is being transported are linked to the alert on the missing child. Should the car be stopped and checked, the authority consulting SIS II will be informed that there is a link to a missing child. This will enable further enquiries to be carried out. Permitting links to be made will mean that SIS II is useful from an operational point of view. However, the legal instrument makes it clear that where there is no authorisation for a link to be viewed, the link will not appear when SIS II is searched. For instance, if there is a link between an alert on a stolen vehicle and an alert on refusal of entry, the UK will be able to see the alert on the stolen vehicle but will not see either the existence of a link or the entry refusal alert, since it does not have access to data on entry refusal.

The Criteria for Listing Persons to be Refused Entry

The UK will not participate in the immigration provisions of SIS II; however the criteria for entering alerts on refusal of entry have been the subject of much debate. The text as amended requires entry refusal alerts to be entered into SIS II on the basis of an individual decision: ie decisions must be made on a case-by-case basis, so that the maximum amount of clarity and accountability is retained. The exception to this rule are the provisions for entering alerts based on UN travel bans, which have already been issued subject to stringent checks.

The Appropriateness of Including Third-Country National Family Members of EU Citizens

A recent ECJ case (Case C-503/03) found that Spain was in breach of EC law when it automatically refused to grant a visa to a third country family member of an EU citizen based on an entry refusal alert in SIS II. The court ruled that a Member State may not automatically refuse entry to a third-country national family member of an EU citizen to the Schengen area on the basis of an alert in the Schengen Information system without further consideration. The Council has taken note of this judgement and it is envisaged that amendments to the text will be made to reflect the ECJ's decision.

The Clarity of Rules Governing Collection of and Access to Data, Including the Desirability of Granting Access to Immigration Data to Police and Asylum Authorities

The UK does not participate in the immigration and border control provisions of the Schengen Acquis, and has no right of access to immigration data contained in the SIS II (covered by the SIS II Regulation) for immigration and border control purposes.

The Government does however believe that there are operational grounds for sharing between law-enforcement the limited category of information on persons who are considered a threat on the basis of public security. In this context, it may be appropriate (subject to strict criteria) to allow limited access to immigration data for law enforcement and asylum authorities. Transition from SIS I to SIS II does not however mean that the UK can re-negotiate the basis upon which it participates in the Schengen Acquis. The UK would not be able to access immigration data for immigration purposes as part of these negotiations.

The Adequacy of Data Protection Rules, in Particular as Regards Data Which May be Transferred to Third Countries

The data protection regime for SIS II has been the subject of much debate during negotiations. The regime envisaged for the system is one which gives responsibility for the supervision of the management authority to the European Data Protection Supervisor (EDPS), and supervision in each Member State to the national supervisory authority (the Information Commissioner in the UK). There are provisions for cooperation between the national supervisory authorities and the EDPS in order to examine cross-cutting issues. There are also stringent rules on monitoring access, ensuring that adequate training is given for those who access the system, and purpose limitation provisions so that data can only be accessed by authorised personnel within the limits of the purposes defined in the legal instruments. The Government is content that these rules allow for a high standard of data protection, as well as ensuring a secure and effective system. There is no provision

in the SIS II text for SIS II data to be transferred to third countries who will not participate in SIS II. Data will therefore not be transferred to third countries. Where it is envisaged that data will be shared with other parties (for instance Europol and Eurojust), the data protection regime has been robustly drafted to ensure that data is not misused.

The Implication of the Plans on Interoperability of EU Databases

The communication on interoperability was published by the Commission on 29 November 2005. The Government supports in principle efforts to improve the efficiency of existing databases, with due respect given to the limitations and constraints upon access. Interoperability or linkage of databases must not result in a situation where information on one database can be accessed without permission via another database.

The United Kingdom's Position on the SIS, Particularly the Need for Access by the UK to Immigration Data

The UK participates in the law enforcement (third pillar) aspects of the Schengen Acquis, but does not participate in the first pillar immigration and border control measures (as set out in Council Decision 2000/365/EC and Council Decision 2004/926/EC). Negotiations on the SIS II legal base are not an opportunity to change the terms of the UK's participation in the Schengen Acquis. Whilst the Government believes that there may be operational merit in accessing and exchanging entry refusal data contained in the SIS II for purposes other than border control (for instance law enforcement or asylum purposes), it accepts that the UK has no right to access immigration data for immigration purposes given that we have not acceded to the border control aspects of Schengen.

13 July 2006

Examination of Witnesses

Witnesses: Joan Ryan, a Member of the House of Commons, Parliamentary Under-Secretary of State for Nationality, Citizenship and Immigration, Mr Jonathan Sweet, Mr Mike Fitzpatrick and Mr Kevan Norris, Home Office, gave evidence.

Q540 ***Chairman:*** Minister, good morning and thank you for coming to give evidence to us again. As you probably know, we have just returned from Brussels where we had two days taking evidence on this subject of SIS II. Some of our questions may relate to what we heard in Brussels but for the most part we shall stick to the list of questions that you were given. This meeting is on the record and is being broadcast. I think you are our last witness in our inquiry into Schengen II. May I also welcome your colleagues: Jonathan Sweet, a longstanding friend of this committee; Mike Fitzpatrick; and Kevan Norris. Is there anything you want to say to start or should we go straight into questions?
Joan Ryan: We can go straight into questions.

Q541 ***Chairman:*** Can I first ask about the UK challenges in the Court of Justice on UK participation in EC borders legislation and ask you what is the current status of that?
Joan Ryan: Your Lordships will clearly know that we have challenged the fact that the UK has not been allowed to participate in the European Border Agency Regulation and in the Passport Regulation. At the moment, we are at the point where these cases are currently with the European Court of Justice. I think we had reached the point where all written information and statements have been submitted. We are now waiting for a hearing.

Q542 ***Chairman:*** May I interrupt you? If I heard you right, you said that the UK is not permitted to take part, but surely it is our choice, is it not, not to take part?
Joan Ryan: The reason that we have not been allowed to participate is because these two Regulations, these two areas, have been seen as Schengen building measures. Of course, we do not participate in all of Schengen and we are not going to drop our borders. As this is seen as a Schengen building measure, that is what we are challenging. What we are saying is that we should be able to participate in European Border Agency Regulation; we already work with other European Union members on border issues and we should be able to participate in the Passport Regulation. Our citizens cross what would be the Schengen border as anyone else, and we are working alongside the European Union in development of our passport. We can see no justification for us not being allowed to participate or for these two measures being seen purely in terms of a Schengen building measure.

Q543 ***Chairman:*** Where does the case stand at the moment? What are the prospects?
Joan Ryan: I am not sure I can really answer that. Obviously we think we have a reasonable prospect.

Q544 ***Chairman:*** Do we have any idea of the timetable for the case?
Mr Norris: As the Minister said, the written procedure is closed and we are now waiting for a hearing date. Written procedure was closed in April of this year. We have not yet been given a hearing date but I would expect it to take place in the first part of next year with a judgment maybe six months after that.

Q545 ***Lord Marlesford:*** Minister, it would be very helpful if you would be kind enough to spell out exactly what it is we are not being allowed to do and in practical terms how that adversely affects British national interests.
Joan Ryan: In terms of the European Border Agency issue, currently for instance we are working with Spain, Italy and Malta around issues of Libya being used as a transit country and the issues of the porous nature of the southerly border, which will be the Schengen border. We are all working together there to address those issues. On the basis of doing that kind of work with our partners in the European Union, we think it is not acceptable that we are not part of this Regulation. We already work together with our other partners. There seems no sensible reason why we should not be allowed to continue to work closely together on Border Agency issues.

Q546 ***Lord Marlesford:*** I am sorry, Minister, I did not make myself clear. I understand the point you have just made because you have already made it. What I do not understand is what, in practical terms, effect this has on the United Kingdom and our national interests.
Joan Ryan: I will ask one of the officials to speak in a moment. From my own point of view, my understanding is that with measures such as the one I have described, we need to be part of discussions and planning and have all the information available around issues such as the one I have outlined because we are affected by that. When people attempt to come in illegally through the border at that part of the European Union, they do not just stay there; they work their way up towards the northern states. We are affected by those kinds of issues. We want to be involved at the very heart of dealing with those issues. This Regulation, as I understand it, puts limits on the level of our involvement.
Mr Norris: As the Minister has said, provision is made in the Border Regulation for co-operation with the UK. I think the other Member States have recognised that our participation and co-operation relating to border control is important and valuable, but because we were not allowed to participate in the Regulation, we do not have full status. For example, we do not have a representative on the management board of the European Border Agency. The management board sets out the programme for the agency. Although in practice we can participate in some of the activities of the Border Agency, we do not have full membership. It is a kind of half-way house. We think that is unacceptable and unnecessary in legal terms.

Q547 ***Lord Marlesford:*** What is the practical result?
Mr Norris: The practical result is that, although we can participate, we have to make requests to participate. Those requests are subject to agreement by the management board. They can refuse. Also, because we do not have a representative on the management board, we do not have the same voice as the other Member States who do participate. It is not that we have been excluded practically altogether but we do not have the full membership status as do the Schengen Member States.

Q548 ***Chairman:*** Does the access that we want from SIS II include alerts on refusal of entry? Does it include some portion of those alerts for instance for someone with criminal convictions and presumed criminal activities? Is that part of our challenge?
Joan Ryan: We have law enforcement access but we do not have access to immigration information within Schengen SIS II. We are asking that where data is available for those refused entry to the Schengen area who are said to be a threat to public policy or public security or to national security, we should have that data because that relates to law enforcement if they are refused for the reasons I have given. We also think that where there is data on those refused entry to the Schengen area who have been subject to measures involving deportation or refusal of entry or removal, if that information is available to other Member States, it should be available to us because it applies to asylum issues and we participate in asylum issues within the European Union. So we want access to that information.

Q549 ***Chairman:*** When we originally signified our opt-out to parts of Schengen, did we specify that these were things that we opted out of or did we express our interest in opting in to them?

Joan Ryan: We accept that, as we are not participating in dropping our borders on some of the immigration side of Schengen in that way, some data we do not have access to, but on law enforcement and asylum issues, we do not accept that. I do not think we ever did specify that we did not want certain things. I think we have mostly been in the position of arguing for the things that we do want rather than talking about the things we do not want.

Q550 ***Lord Avebury:*** My question goes back to an earlier issue we were discussing. That is that if we do not have any say in the amnesty that has been granted by some European countries allowing large quantities of people to remain within the European Union, have we found in practice that this affects us directly in that, for example, when the 700,000 people were given an amnesty in Spain, some of them would finish up in the United Kingdom later on? Is that one of the reasons why we need to have a say in these issues?
Joan Ryan: I think that strikes me as a very good reason why we should have a say in these issues. There was a discussion on these grounds at the informal Justice and Home Affairs meeting in Tampere in Finland in September. A lot of Member States around the table get very upset at other Member States giving amnesties because they feel it is a very strong pull factor and it does not help us as a European Union together in trying to deal with these issues. I think there is merit in the point you have made and it is certainly one we would recognise.
Mr Sweet: May I add that I am not sure that there is any particularly important strong pull factor in relation to people coming specifically to the United Kingdom as a result of mass regularisations of the sort that have been described. As the Minister said, it is clearly a concern for all Member States generally and a number of other EU Member States have actually engaged in this discussion precisely because they are worried about the potential movement of people from one Member State where they, say, might have been regularised into others. That is obviously particularly true for those who have contiguous land borders.

Q551 ***Chairman:*** Can I ask a question that will probably apply to quite a number of questions we ask? Is the Irish position identical to ours and is the Irish wish list the same?
Mr Sweet: Essentially it is, yes. The policy that has developed in relation to these issues, in part because our relationship with Ireland and the common travel area, means that essentially their policy approach on these issues mirrors ours.

Q552 ***Lord Corbett of Castle Vale:*** Minister, your colleague Mr Norris said that one of the practical effects is that when we want to access information on the immigration side, we have to make requests to the management board. How many times have requests been refused, if that has been the case, and can you give us a couple of examples of what we were not allowed to have if that has happened?
Joan Ryan: I am not sure I have a practical example for you.

Q553 ***Lord Corbett of Castle Vale:*** Have any requests been refused by the board?
Mr Sweet: I am not sure that there is an example.

Q554 ***Lord Corbett of Castle Vale:*** Has the board on occasions said, "No, you cannot have it"?
Joan Ryan: This has not happened yet.
Mr Sweet: This is in relation to operational activity that the borders agency is undertaking and projects of one sort or another. On those occasions to my knowledge where the UK has asked to participate in those joint operations, it has always been able to do so. We have not, to my knowledge, had an occasion where the UK has requested the opportunity to participate in a joint operation and it has been refused. I think most Member States recognise that the UK has a great deal of practical experience that it can offer to these sorts of exercises.

Q555 ***Lord Corbett of Castle Vale:*** I am sorry to pursue this but it was given as an example in response to Lord Marlesford's question as to what are the penalties for us not being wholly in it. In practice, the management board issue does not matter, does it, in that sense?
Joan Ryan: It has not so far in a sense, but that does not mean it would not in the future.

Q556 ***Lord Corbett of Castle Vale:*** I understand that.
Joan Ryan: Also, it does not in any way take away from the fact that we feel in principle we should be allowed to participate in this way.

Q557 ***Lord Corbett of Castle Vale:*** It is also a two-way street, is it not? We have information which would be useful to some of our partners from our own experiences?
Joan Ryan: Yes, indeed.

Q558 ***Baroness D'Souza:*** Minister, to what extent has the Government already arranged, or is planning to arrange, access to those alerts other than through the SIS II system? In particular, what are the provisions of any agreements or informal

arrangements with Member States to obtain access to such alerts?
Joan Ryan: At the moment, that is something we are looking at. The Government will explore alternative methods of sharing information on third country nationals who are refused entry for security purposes. We will look at mutual information-sharing agreements with other Member States, possibly through a bilateral exchange of information, but at the moment that is something we are looking at and hoping to make some progress towards some firm ways forward that we can pursue with other countries. We are no further than that at the moment.

Q559 ***Baroness D'Souza:*** When might you expect to arrive at those agreements or is that really pushing it?
Joan Ryan: I do not have an answer to that at the moment. As I say, we are just starting to look at that as a way forward.

Q560 ***Lord Avebury:*** Would these arrangements, if they do come off, result in conditional access by our officials to SIS II alerts on the computer system?
Joan Ryan: It is indirect access rather than conditional access. It is making an agreement with somebody else who may have that information and how they will exchange that information with us, but we do not expect rapid progress on that issue at the moment, it is true to say.
Mr Sweet: There is of course sympathy from some Member States towards the UK's request to have access to these data, but quite often one comes up against the fairly fundamental point, which is that other Member States suggest that if we want full access to all the information that is available on Schengen information systems, then the short simple answer is for the UK to participate fully in Schengen.

Q561 ***Lord Corbett of Castle Vale:*** Given that the UK opted out from the negotiations on the SIS II immigration data Regulation, to what extent did the UK nevertheless take part in the discussion, informally perhaps, of this proposal? What positions did we advocate and how influential were we?
Joan Ryan: It was more than informal. During the UK presidency, we chaired the Schengen Acquis Working Group. We have attended and participated in all working group meetings, so we have been very involved. We have not been successful in pursuing all of our objectives in terms of some of the discussion we have just been having in that indirect access and entry refusal data for asylum purposes issue; we were not successful there. However, that is not to say that we did not have some successes on some issues. We had a number of objectives in terms of this working group: inclusion of biometrics, for instance, and we had some success there; flexibility of the use of the system; scanned copies of European arrest warrants on the SIS II; extended access for Eurojust and for Europol to help them better to fulfil their tasks; and the mechanism for oversight for data protection, which I know is an issue that this committee is always concerned about; and a mechanism that is independent of the Commission, preferably a single structure. We are broadly happy with the outcome of the negotiations on these points. The committee is aware that we have been unsuccessful on some key issues for us.

Q562 ***Lord Teverson:*** Minister, to clarify something in my own mind here, this question we have just heard relates to a Regulation. Schengen is now part of the Acquis of the Community, as opposed to a separate agreement. I presume, in terms of the Council of Ministers, that in all Regulations clearly the UK is able to participate or is a participant in all legislation as part of the legislative process. There is no longer a separate Schengen Council group that votes on legislation presumably, or have I got this wrong?
Joan Ryan: I will ask the officials to come in on this in a moment. My understanding is that because we opt out and we do not opt in to the whole of Schengen, then we are not allowed to participate in all these Regulations.

Q563 ***Lord Teverson:*** I am talking about the legislative process in terms of voting in the Council of Ministers.
Mr Sweet: Essentially, as you say, the Schengen Acquis was incorporated into the body of the EU and there is, in that sense, not a separate mechanism as such. When it comes to discussing particular proposals which might be brought forward that relate to aspects of the Schengen Acquis, then those are discussed in the Schengen Acquis Working Group, for instance, which is within the Council structure. Clearly, in relation to each individual instrument, if it is an instrument which, if one accepts the Council Legal Service analysis for example, builds on a part of the underlying Schengen Acquis into which the UK had not opted, then we do not participate in that instrument. We can contribute to the discussions—we are still in the working group and we do contribute to the discussions—but we will not, at the end of the day, formally be a party to that instrument.

Q564 ***Lord Teverson:*** Forgive my newness to this committee. When it is a Regulation, which is a legislative instrument within the European Community depending on the pillar, I had not understood that all Member States were not able to participate in actual Regulations. It may be that working parties follow on from Schengen but, in terms of the legislative voting in the Council of Ministers, are we actually excluded from that?
Mr Sweet: Yes, we do not participate in the Regulation itself. This is a particular example. There are two instruments for the Schengen Information System. One is a third pillar Council Decision, in which we do participate; the other is a first pillar Regulation. Because we have not chosen to participate in the underlying part of the Schengen Acquis, which deals with those immigration aspects, then we do not participate in that Regulation.

Q565 ***Lord Teverson:*** That is part of the Treaty of Amsterdam, is it?
Joan Ryan: The debate we are having is that some of what is in the first pillar relates to law enforcement, not just immigration. Therefore, we think we should be able to participate in the law enforcement aspects of it.

Q566 ***Lord Teverson:*** I understand the participation issues. It is the core legislative issue that I had not realised.
Joan Ryan: Other Member States say, as Jonathan said, that the solution rests with us because we can opt in to the whole of Schengen if we wish. It is simply because we opt out that we are not able to participate in those Regulations that relate to parts of Schengen we decided not to participate in.
Chairman: I think to some extent we are getting into this rather complicated area of distinguishing between first and third pillars.

Q567 ***Lord Dubs:*** I think you have probably answered my question. My question is about what the main objectives were of the UK Government in negotiating the third pillar of the SIS II Decision. If you have not already answered that, I would welcome an answer, together with how well we can achieve those objectives and on which points did we have to compromise or relinquish our objectives. I think that was a third pillar answer.
Joan Ryan: I think I answered that.

Q568 ***Earl of Listowel:*** Minister, can you say who is responsible for the delay in the application of SIS II, which has caused so much concern to the new accession countries? Has the Government now come to a final position on whether it will support the extension of the current SIS to new Member States in the meantime?
Joan Ryan: I think our view is that no single body is responsible for the delay. There are three main causes. One was the delay to the preparatory work required at the French site. One was the legal challenges to awarding the main development and network contacts. The third main delay was to do with the legal basis that has taken five months longer than anticipated. I think there would also be doubts as to whether, had things all gone to plan, which of course they have not, all Member States would have been ready to join themselves on the original timetable. There is a number of reasons for the delay. Though it would be easier to be able to point the finger at one single body and reason, I do not think it is possible to do so. In terms of what is now called SISone4all, to be candid with the committee, we have had concern about creating SISone4all and expanding SIS to accommodate fundamentally the 2004 A8 accession states. We understand that this is a big issue for them and part of the commitment they made to their populations of the countries on accession. We understand that they are very frustrated at the delay. As for our own view, we have had concerns about the technical feasibility of it, though we understand that, after consideration, it is technically feasible. I will ask one of the officials to comment on that in a moment. That is about as far as I can go on the technical information, but we understand that it is being judged to be technically feasible to do this. We are not going to oppose SISone4all. We cannot in fact stop it, even if we did. We are not going to oppose it but we are not ourselves looking to participate in SISone4all. Our concern is that focus on SISone4all would further delay SIS II. So we have made very strong noises in various meetings at different levels, both at political and official level, about those concerns and that SISone4all will not be worth it if it delays SIS II to any significant way, and there is a question of whether SISone4all is worth it if it is so close to SIS II coming on stream. Those are all decisions for those who will participate in SISone4all. We have made clear our concerns and I think those concerns have certainly been listened to. Obviously, I think there will be consideration of this issue on the 4 and 5 December, which is now next week, at the Justice and Home Affairs Council in Brussels. We want to object. We have had a lot of conversations. We do have some concerns. We have sought reassurance on those concerns and we do think those concerns are being taken on board. That probably sums up our position. We are fully committed to delivering SIS II, and to plugging into that as early as possible, by 2010.
Chairman: Minister, I should say we did not have an opportunity to question the Portuguese about this in Brussels, but I think the concerns you have referred

to are certainly reflected in the comments that we had from the Commission and others both on technological grounds and, most particularly, on the risk that delay will be further increased, but it is very helpful to have your reaction to it.

Q569 ***Lord Avebury:*** I wonder if you have thought of any assessment of the extent to which our entry to those parts of SIS II to which we will have access in 2009 is likely to be delayed by the diversion of effort of the SISone4all and whether, in discussions with the accession states, it has been pointed out that this diversion of effort may be to their detriment as well in that they will not have full access to the facilities of SIS II until a later date than would otherwise have been possible?
Joan Ryan: As to SISone4all and whether or not that will cause further delay to SIS II, that is a concern about which I do not have an assessment. I have designated Mr Fitzpatrick as our technical expert who will address that as far as we are able. You mention 2009. Because of all the problems with SIS II, the likely plug-in date for us is 2010 at the moment. We need to be very aware of that. We are already conscious of the delay.
Mr Fitzpatrick: The current impact assessment which will go before the meeting of 4/5 December suggests that the impact on the delivery of SIS II will be five months, but that is predicated on the current SISone4all timetable, which, as the Minister has indicated, we do not think will be done, so it is likely that were SIS one for all implemented, the delay would be more than those five months. On our current timetable, a delay of five months to the delivery of SIS II centre would not impact our delivery. However, should that creep, we may well be affected.

Q570 ***Baroness D'Souza:*** Minister, has the Government arrived at any conclusion about the options for the agency that will operate SIS II in the future? In particular, would the Government support or oppose management of SIS II by Europol or by Frontex, the European borders agency?
Joan Ryan: We are pleased that provisions of the draft legal text will set out the role and responsibilities and funding of the proposed management authority. We do not want to pre-empt the impact assessment that will have the substantive analysis of alternatives to setting up an agency to be responsible for this long-term operational management of a central system. I suppose the answer is 'no' at the moment.

Q571 ***Baroness D'Souza:*** As a supplementary, the idea that came up before that there would be a new cross-pillar agency is not something that you are going ahead with full steam?
Joan Ryan: We are not not supporting that, no. I would not say we were not supporting that. We are happy for that to continue to be looked at but we want to see its impact assessment before we make a decision as to where we stand on that.

Q572 ***Chairman:*** As I understand it, but perhaps I do not understand it, the idea of the agency arose because of unhappiness at the thought of the Commission running this. Do we share those worries about the Commission being in charge?
Joan Ryan: I think I would say we are keen to have the impact assessment and then consider, as Baroness D'Souza said, the cross-pillar agency and look at that. I am certainly not being negative. I am just saying we are not at the stage where we have that position at the moment. We are just keeping the options open but you are absolutely right, Lord Wright, about the reasons why this has been looked at and the concerns that Member States have expressed about who should be in this position, who should be in the management position over this.

Q573 ***Chairman:*** I should say that since many of us I think round this table, and indeed in this room, have experience of the difficulties of running major IT operations, we will look with great interest to see who is chosen to run this agency because I think probably the number of people or agencies in this world who are capable of running IT operations as complicated as this is probably very few. That is not a question to you so much as a personal comment.
Joan Ryan: I think it is a very major and important decision. That is partly why I do not have an absolutely clear answer at the moment precisely because of what you have just said, Lord Wright. That is why I think the impact assessment is so important so that we have that basis on which to make an informed decision about something that is going to be very important for us.
Mr Sweet: We do expect that impact assessment to contain a substantive analysis of alternatives to the agency. It is as a result of that impact assessment that we would be able to judge the comparative merits of different models for the management of the system,

Q574 ***Earl of Caithness:*** I would like to ask a supplementary on that before I get on to my question. As I understand it, the Commission are looking at five different options. What is the timing of their work and do you have any input into it?

Mr Sweet: Offhand, I do not know whether there is specific timing but we can check.

Q575 ***Chairman:*** Minister, perhaps I could say in that context that if at any point, particularly after you receive the transcript of this meeting, you or your colleagues think of points that ought to be sent to us as supplementary evidence, we would be very happy to receive it.
Joan Ryan: Certainly, I think we should do so in answer to that point.

Q576 ***Earl of Caithness:*** Minister, can I have an answer to my question? What degree of public and parliamentary scrutiny and control will apply to the decision to exchange SIS II data with Interpol, including the decision as to which other Interpol countries will be able to access that data?
Joan Ryan: We will only exchange certain data with Interpol, as you are no doubt aware. That will be relating to lost, stolen or misappropriated passports only. The draft Council Decision contains a draft Council declaration regarding the nature of the agreement to be reached with Interpol. This declaration sets out the conditions that must be satisfied in reaching this agreement. The legal texts themselves establish parameters for the decision on sharing data with Interpol. Any of those countries that take part in Interpol are eligible to have access to the data transferred from SIS II to the Interpol database, but only if they meet what are described as stringent data protection and security criteria. In effect, the requirement will act as a significant filter that will limit those countries with which data can actually be shared. An important point is that the transmission of data on these lost, stolen or misappropriated passports to Interpol will be subject to the consent of the Member State who entered the data in the first place. I think there is a protection there. Obviously, we will seek to keep this committee and Parliament in general informed of the progress on the agreement as it is being developed.

Q577 ***Earl of Caithness:*** On your last answer, how are you gong to keep us informed because the secrecy regarding SIS I is something to be believed in comparison to quite a lot of other organisations. Minister, are you happy with the data protection agreement with Interpol and do you know which countries are likely to have access to this data?
Joan Ryan: I think there are, as I said, stringent data protection and security criteria. I am not concerned that that is going to be a problem. As to which countries, I am not sure that I am the best person to answer that. Kevan can give us a little bit more detail on which countries will have access to that outside ourselves.
Mr Norris: I am not sure that I can add very much. My understanding is that any members of Interpol, any countries belonging to Interpol, will have access to data. It is an exchange via Interpol to the states which participate in Interpol.

Q578 ***Chairman:*** Would the exchange with Interpol be via Europol?
Mr Norris: I think it is a direct exchange via Interpol to my understanding. It is not going via Europol.

Q579 ***Baroness Henig:*** This is a short and straightforward question. What is the likely timetable and content of the Commission report on the technology for 'one-to-many' searching on biometric data?
Joan Ryan: I am not sure there is quite as short or direct an answer. The Commission will produce this report as soon as it considers the necessary technology is ready and available. We would be disappointed if it is not produced by 2009.
Baroness Henig: You are projecting somewhat ahead.

Q580 ***Lord Avebury:*** I must confess I am a little bit surprised by that answer. The technology for one-to-many searches is already available and, as a general matter in IT technologies, there are one-to-many searches which are conducted on a regular basis. I wonder if there are any particular difficulties arising from this particular set of data which mean that this is taking far longer than it would in, say, a commercial environment.
Joan Ryan: I think some of the issue is about availability and readiness and also we raised concerns with officials about data quality assurances and accuracy of the technology. I know the technology is available but availability and readiness are features.

Q581 ***Lord Avebury:*** I am not suggesting you should go into the detail here; it would not be appropriate. I would find it interesting if we had a slightly amplified note on why the delays should arise from the conduct of one-to-many searches when it is a common operation in the commercial environment. Let us not continue that at this moment.
Joan Ryan: As you have mentioned one-to-many, I think there is an issue about one-to-many. The use of the term in this context is a bit misleading. I am looking at Mr Fitzpatrick because I have had this conversation with him and I am hoping he will explain why it is misleading.

Mr Fitzpatrick: I think the timing of the report is a matter for the Commission and the resource they allocate to it. Our suggestion is that we would be disappointed if it was not ready by 2009 but we will obviously inquire of them whether or not it can be delivered earlier than that.
Joan Ryan: Some of what we are talking about is the use of the photograph; it is verification rather than a one-to-many search. I am not sure that has illuminated anything for your Lordships at all. You suggest that you would find a note useful and we will do just that.

Q582 ***Lord Avebury:*** Thank you, Minister. My next question is this. As regards these one-to-many searches, what public and Parliamentary scrutiny will there be of the decision to apply this functionality and what controls will there be on the process of applying it? What would happen if one or more national government or parliament objects to the idea of applying this extension of this functionality of the system?
Joan Ryan: The SIS II Decision states that identification using fingerprints will be introduced as soon as it is technically possible. Technically that can include the issues we have already talked about, not just technologically but technically possible. Further decisions are to be made concerning technical details. Once the Commission's report has been published, as I understand it, Member States will need time to look at the findings in the Commission's report and the European Parliament will also need to be consulted at that stage. It is only then if all Member States are satisfied that the use of fingerprints for identification will actually be permitted. Key players such as the Commission, the Legal Service and the Council, will need to be satisfied that necessary safeguards are in place regarding accuracy and data protection before Member States could start using fingerprints for identification. That is in process at the moment and we are not there because we await the Commission's report. We will get the report; we all need time to look at it. The Commission, Legal Services and the Council have got to be absolutely satisfied that the necessary safeguards are in place and we will need to involve Parliament through these normal scrutiny procedures.

Q583 ***Lord Avebury:*** So there will be a motion before Parliament to extend SIS II to one-to-many searches?
Mr Norris: Looking at the text of the SIS II instrument, the legal precondition for the exercise of this functionality is that the Commission should present its report; once that report has been presented, that has cleared the legal requirements and then the functionality legally is available. That is obviously subject to the technology being there.

Q584 ***Chairman:*** But it is up to our Government to put the motion before both Houses for negative or affirmative resolution? How will that be accomplished?
Joan Ryan: The normal scrutiny that I am referring to is the scrutiny with our select committee procedure.

Q585 ***Chairman:*** Minister, I make a comment rather than putting a question here. We were struck during our visit Brussels by the extent to which a decision on whether to opt into third pillar measures would primarily be based on the Government's assessment of the advantages for us, for the British, but we were also struck by the fact that an opt-in by Britain should have considerable advantages for our European partners in terms of the exchange of information that would become available to them. I only make that point not to argue one way or other but it is a consideration which I would hope the Government will take very strongly into account.
Joan Ryan: I think any discussion we have at Council level and with partners in the European Union is that this is very much a two-way street and that is the whole purpose of working in partnership; benefits go both ways.

Q586 ***Lord Avebury:*** Could we turn to the question of whether or not we opt into the Court of Justice's jurisdiction on third pillar matters? Could you tell the committee on how many occasions and what was the most recent one when the Government refused to review that decision and what are the reasons for the current policy of not opting in? When do you think that the decision will next be refused? Can you explain how the interpretation of third pillar measures can be assured EU-wide when some members do not opt in?
Joan Ryan: At the moment, we have great concerns that any extension of the court's competence would result in cases taking longer to get through the system than they currently do. In terms of reviewing the European Court of Justice's jurisdiction to third pillar matters, I think it is true to say that was last considered during the detailed discussions around the Constitutional Treaty. Of course, if Article 42 was to be brought into use, then again it would have the same effect in that it would extend the court's competence in that way. As your Lordships know, that is an issue that has been on the agenda through the Finnish presidency. We very much think, after Member State contributions at the informal meeting at Tampere on the issue of passerelle Article 42, that

the current debate on that issue is probably closed. We will know that next week at the Council. The issue is not therefore being reviewed in that sense now. The next time I think it will be reviewed will be in the second half of 2007 when the period of reflection on the Constitutional Treaty comes to an end.

Mr Sweet: May I add one point of clarification? I am sure Mr Norris is better able to explain it than I am. When one uses the term 'opt in', this is not an opt-in in the more traditional arrangements as it were in relation to the UK's position. As I understand it, and again Mr Norris will correct me, the provisions in Article 35 of the Treaty actually specify that a Member State may, by way of a declaration, decide to accept the jurisdiction of the Court of Justice. Just to be clear, this is not something that is the usual, as it were, opt-in arrangements. I wanted to be clear on the term.

Chairman: Thank you. That is a helpful clarification. It clarifies something that I had clearly misunderstood.

Q587 ***Lord Harrison:*** Minister, this is a question about resources. The Crown Prosecution Service suggested to us that their workload in respect of extradition and dealing with the European Arrest Warrant might double or triple when SIS II comes in to the United Kingdom. Do you share that view? If you do share that view, is the Government prepared to double or triple resources? Beyond that, are there other resource implications beyond that of the EU framework?

Joan Ryan: I certainly share the view that the Crown Prosecution Service has stated that there will be an increase in extradition traffic, should we call it. I also think that is a very good thing and one of the outcomes we would want from the European Arrest Warrant because, of course, that will mean more people are being brought to book to face justice, to be prosecuted and to be tried for any offences of which they may be accused.

Q588 ***Lord Harrison:*** The question is about resources.

Joan Ryan: I think there will be an increase in traffic. The development of the European Arrest Warrant and the introduction of SIS II will also bring efficiencies in some areas. There will be some balancing because of that.

Q589 ***Lord Harrison:*** Is it not true in that case that efficiencies anyway could be brought in at any time? The CPS is saying there could be a doubling or a tripling of the workload, however much you seek to find some savings. Is there an implication of resources? What I am asking you is if you are alert and ready and able to respond to that at all?

Joan Ryan: We are seized of the issue of resources, so, yes, we are aware that there may be resource implications and we are alive to that issue. Some of the efficiencies that I am referring to that will come with SIS II and will bring about operational changes is ongoing work as to how much efficiency will be brought about. At the moment, we do not have an exact picture of what it will be.

Q590 ***Lord Harrison:*** My supplementary question implied that there is always active work being done order to introduce efficiencies into any operation. I had not understood a qualitative difference of that kind was being done. I understand it is going to be a quantitative difference in terms of a doubling or tripling and that in turn suggests that you would require resources to be raised at least.

Joan Ryan: I am not trying to avoid answering you, Lord Harrison. I am saying that we are aware of what the CPS has said. We are aware and welcome the increase in European Arrest Warrant extradition traffic and we are seized of the issue of resources. We are aware that Rob Wainwright of the Serious and Organised Crime Agency raised status in his evidence and that he is satisfied that the Home Office was seized of this issue. So we are looking at it and it will come into our planning.

Q591 ***Lord Harrison:*** Have you identified further resource implications that might be beyond the immediate area of extradition and the European Arrest Warrant because of entry into SIS II?

Joan Ryan: I do not have any details for you on that but the whole issue of what impact it will have for us when we plug into SIS II and how much impact that will have on resourcing requirements is an issue that we keep under constant review. As I said, plugging into SIS II is now 2010, so planning for resources on the basis of something that is subject to movement is not an exact science or a precise exercise. We would not want to identify resources, and we certainly would not be able to just leave them sitting there and not use them because something did not happen. It is a slightly more complex procedure than saying, "This is going to happen, so we need these resources".

Chairman: Minister, thank you for that reply. When you look at the transcript, if you have anything to add to that and are able to put any more flesh on that answer, we would very much welcome it.

Q592 ***Lord Dubs:*** Does the Government now have a firm view as to whether UK legislation will have to be changed in order to implement SIS II?

Joan Ryan: We do. We are satisfied that no further legislation is required. My officials have consulted widely during negotiations. We have not been advised of any gaps in existing legislation. Many of the provisions refer back to relevant national law on subjects such as data protection. They are not seeking to create harmonised EU-wide provisions, so we are satisfied that, yes, we do not need further legislation.

Q593 ***Lord Marlesford:*** Minister, what has been the total cost of SIS I to the British taxpayer so far? Can you give us, with some practical examples, the way in which we have had an advantage being part of SIS I?
Joan Ryan: I might need to write to the noble Lord on the precise costs, I do not have that to hand. Maybe I misunderstood the question, but I understood we were going to talk about savings. Having referred to that, I was simply going to say that when the UK negotiated to join parts of Schengen, including SIS I 1999 to 2000, of course we did not know about SIS II then, it had not been proposed. It is difficult now to estimate how much of the SIS I costs will eventually benefit the SIS II programme during its lifetime.

Q594 ***Lord Marlesford:*** That is why I did not ask the question.
Joan Ryan: I could not have answered that either. That is a very good point. I would appreciate being able to look a little more closely at that. I would be very unwilling to give the Committee figures which I had not had a good look at, but I will come back to the Committee on those matters.

Q595 ***Lord Harrison:*** Minister, your officials told us that we are paying for our SIS II subscription pro rata with the other Member States, but I wonder whether you can justify that and whether we will receive any proportion of the information which is available to those States ?
Joan Ryan: I read the transcript, compared it with my information, and I am pleased to say it did marry up which is always a bit of a relief. Yes, I am aware that the annual cost is half a million pounds for our SIS II subscription, and then we have in the order of three to four million pounds a year operational running costs. In terms of paying our subscription, my understanding is that set-up and running costs are determined by the infrastructure which we need for the system itself rather than by the data which is held in it. Our contribution, which is based on GDP, on a formula which comes out at some 18 per cent, which is our contribution, comes out at half a million pounds. I guess the point your Lordship is making is if we are not getting access to all the data, why are we paying the full sum? I think that is a really valid question to ask; it is certainly one I have asked having seen the original questioning. I am sure the answer is that it is about paying for this infrastructure which we would be paying for for whatever data we got out of it. I also think there is another point beyond that which is perhaps a more political point and that is we want to constructively engage with the Commission on the ways in which we will access all the data. I am very determined about that programme, particularly in relation to being able to use the immigration information for law enforcement purposes; I think that is very important for us. That is the debate I am pursuing most strongly. I am not sure that would be helped if I started talking with them about this half a million pounds, especially as I cannot find really solid grounds in relation to the amount of data.

Q596 ***Lord Harrison:*** I wholly agree with you about that, but you do acknowledge that we are missing out on information we might otherwise obtain?
Joan Ryan: I do entirely, and part of my brief is to access exactly that information we have been discussing today which I think we all think would be very beneficial to us and would be part of the two-way street which we have referred to.

Q597 ***Lord Marlesford:*** Following that up, Minister, have you been at least able to identify, and if so will you tell us, where the obstacles to our full participation in SIS II information lie? Is it the Commission or is it individual countries and if so, which countries?
Joan Ryan: I think we discussed this the last time. Originally we thought we were going to be able to participate in all the data that we discussed which we wished to have access to. There was a decision—perhaps Mr Norris will correct me if I stray on this because it is an important point—by the Council Legal Service which ruled as to whether we could participate in some of the data and whether or not it was part of the Schengen building measure. That is my understanding of why we do not get to access some of these immigration data in relation to law enforcement because it is classed as a Schengen building measure and that is a ruling by the Council Legal Service. However, I think it would be true to say that there are Member States that would think that you should participate fully in Schengen if you want all the data.

Q598 ***Lord Marlesford***: Which ones?
Joan Ryan: I do not know if I can name individual countries in that these are often informal discussions, and obviously I am also working very hard to build our case and win support for our case

from other Member States. I do not want to lock them into a position and then not be able to get them back out of that position and win their support for our position; that would not be the most sensible way forward. Member States do change their positions on things and they can achieve movement, so I wish to be diplomatic about that.

Q599 ***Lord Marlesford:*** On the legal services barrier, do the British Government's legal advisers believe that this decision had legal validity?
Joan Ryan: Yes.
Mr Norris: If we look at the court cases we have at the moment, the Council has acted on the basis of advice which it has received from the Council Legal Service, and the UK Government has acted on the advice it has received from lawyers here. We disagree with the analysis which the Council is putting forward on the basis of the Council Legal Service advice and that is what the court case in Luxemburg will determine.

Q600 ***Earl of Caithness:*** Minister, we had some quite interesting answers to this question over the last couple of days and I am looking to you for great clarity and precision on this. What is the Government's view on the process of the negotiation and management of the SIS II project? Let us go back. We knew in the late 1990s there were going to be new Member States. We knew that SIS I, the Schengen Information System, needed to be updated. We are now trundling along eight years later, the project is late, some of the contracts were awarded before the legislation had even been proposed, there had been no impact assessment, there is no explanation of the text of the legislation and there are no statistics of any worth from SIS I to base SIS II on, what is your view of all of this?
Joan Ryan: I understand that consultation did take place in relation to SIS I and, because SIS II has developed from that, the view was there was no need for an impact assessment, and all these matters were dealt with as SIS I was being agreed to. However, you may be aware that we have called for greater transparency from the Commission during the development of SIS II, so I think that indicates we have had concerns and we want greater transparency. More generally, in terms of the handling of future legislative proposals, the Commission has recently published a communication on the evaluation of justice and home affairs policies and we broadly welcome the Commission's proposals. We have long called for proper evaluation of the impact of EU measures to identify policy areas where action at the EU-level is workable and cost-effective. I think there are issues around transparency and evaluation. The Commission and the Justice and Home Affairs Council are starting to address those issues.

Q601 ***Earl of Caithness:*** Minister, is it not a bit late to call for transparency when it has been in the hands of the Council since 1999 and stopped being the responsibility of the French who were running the Schengen office? It came within the EU ambit and became the responsibility of the Council to provide information. Is that not something you ought to have been attending to? Let us go back on another point. In the written evidence from the Commission they say: "The current SIS has proved its efficiency and added-value" but there does not seem to be any evidence to justify that. Have you got evidence to justify that which has not been given to us?
Joan Ryan: I am trying to think of what I would refer to as to the various documents we have seen.
Mr Fitzgerald: We have statistics about the number of arrests that result from European Arrest Warrants which are carried by SIS I in other countries. We could certainly present that evidence but that is current information. I am not sure that any analysis has been taken comparing that with the number of cross-border arrests which occurred prior to the implementation of SIS I. Obviously that was not a concern for us, we were clearly interested in how SIS I might improve things for us when we had to implement SIS II.
Joan Ryan: That is why the evaluation issue is important to us because we will plug into SIS II. Clearly there are valid points about the need for sound evaluation. I think that has generally been the theme at the Councils I have attended, and it is certainly part of The Hague Review programme that evaluation is an important issue which we need to pay some more attention to. You made a valid point but we do not participate in SIS I.

Q602 ***Lord Teverson:*** Let us move on to the last section, the Treaty of Prüm, which, as you know, Minister, has been concluded but, as we understand, the German Presidency wishes to put on the agenda to extend as an EU-wide initiative. We are interested as a government that supports this. If the Treaty is integrated into the broader European framework would we become a part of it? What implications would that have for SIS II and the related data protection regime?
Joan Ryan: Our understanding of what you say about the position of the Germans in relation to the Prüm convention in their Presidency is correct. We believe there are potential benefits for signatories to the Prüm convention, so we are looking at that very actively at the moment. I am sure we will come back to that in future sessions. It would seem sensible to allow all of the Member States to share those benefits.

There are also aspects of Prüm which are still under careful consideration, and there are some details on which we have concerns and would certainly want those addressed before the UK would be able to adopt the Treaty. As I understand it in relation to data protection, the provisions of Prüm generally defer to national legislation, so the data protection measures in Prüm would not in any case lower the national provisions which we have already got in place. Prüm and SIS II both facilitate the sharing of data for law enforcement purposes, but they can also work independently of each other. I hope that answers the question.

Q603 ***Lord Teverson:*** I am interested that you used the adverb "actively" for looking at joining Prüm, but presumably the Government made a decision not to be one of the initial states in the Treaty of Prüm. Has anything changed, or is it a "wait and see" how it works issue?
Joan Ryan: I think we did "wait and see" a little bit and, also, the world has changed as well. On things like the need for greater co-operation on law enforcement across borders and between countries, I think the need is great. We have done a lot of work with the European Union on these issues, particularly during our Presidency. I do not want to over-claim for any particular measure of the Prüm Treaty or anything else, but we led on the counter-terrorism strategy. I think all these measures, the way we worked with our European partners during the summer, during the alleged airline plot, show us the need to work together on these matters of law enforcement and that is the focus of the Prüm Treaty. Yes, we did "wait and see", and, yes situations have changed, so we are actively looking at signing it eventually.

Q604 ***Chairman:*** Minister, are we right in thinking that we were not invited to take part in Prüm, were we?
Mr Sweet: I am not sure I can answer that question as I was not involved in the process at the time. Essentially, as I understand it, it was a process which evolved out of bilateral discussions between a number of Member States which came together to discuss these issues and produce what is now the Prüm text. They have certainly made it clear since then, if not at the time, that they would very much hope that other EU Member States see the benefits of participating in that. That is precisely why we are now looking very actively at doing so.
Lord Teverson: Chairman, the reason I make that point is, although that might be the case, I cannot imagine that we did not realise those bilaterals were taking place and I cannot imagine if we had shown an interest we could not have been involved.

Q605 ***Lord Foulkes of Cumnock:*** Chairman, as you know, and I will confess to the Minister, I have been plunged into this Committee at rather a late stage, so if my question is not too relevant I hope, Minister, you will forgive me. Listening to the answers to Lord Caithness's question, I wonder if the Minister thinks that progress is being made sufficiently quickly to deal with the potential dangers and threats. Is she happy that this is being dealt with with sufficient urgency?
Joan Ryan: One of the things I have personally spoken on to the Justice and Home Affairs Council and one of the directions we are very keen to push on is that we want to see more practical co-operation on the ground, Member States working together, and good evaluation. That has been one of the reasons why we are saying we do not want to be focusing and spending a lot of time on these issues between the first and third pillar. We want to go from where we are now and work on some of these very crucial issues. Yes, I think we have seen some very good progress on the ground but, equally, there are areas where that is not the case. I think focusing on practical co-operation and working together on matters which affect all Member States, matters around illegal immigration, organised crime, the need for effective counter-terrorism strategies, are issues which matter to all European citizens. The more work we do on those issues and the more we can demonstrate the real benefit of that work then I think the more confidence European citizens will have that the European Union and our partnership and the work we do there is relevant to them. I think we have made some very good progress but there is an awful lot more to do and it needs to be focused on.

Q606 ***Lord Foulkes of Cumnock:*** What do you think is delaying progress—and I do not want to follow Lord Marlesford's line and ask you to identify particular countries—but is it because of opposition from particular countries or is it some of the questions that we have been raising earlier in the debate about particular issues which cause concern about individual liberties and freedoms and the kinds of things that Lord Avebury was going on about?
Joan Ryan: I think different countries and different groups of countries often have different pressures on them, different national priorities and different comparatives. For example the new Member States from the 2004 intake and the importance of them being able to plug into SIS I and the commitments they gave to their populations about the dropping of the internal borders and concerns that they are not on a level playing field with other Member States, they are very important issues for them. Equally, what is very much the focus for us is counter-terrorism law enforcement and dealing with illegal immigration. I

think all Member States are concerned about these issues but for some they are much more the immediate focus than perhaps for others. Sometimes it is determined by how long you have been there or what is happening to you. Spain, Italy and Malta are desperately concerned about illegal immigration and the problems they are experiencing there. There are a number of reasons why but I am not sure it always has got to do with how the balance in your own country manifests itself between individual liberty and issues of security. I think we talk a lot about them. Interestingly, although they are issues for countries, when you get to the Justice and Home Affairs Council one of the most interesting things is talking about the practical measures we take on the ground and how much scope there is for us to work together, and I think it is right. One of the good things about The Hague Programme Review is this focus on moving to working together even more strongly on this approach. I think we will see a real benefit. Perhaps then when we come to discuss some of the other issues, like who is involved in what and the balance between various issues of security or liberty, I think we will have a much more grounded and sensible discussion on all of those issues if that practical co-operation is strengthened and is underpinning the relationship.

Q607 ***Lord Avebury:*** At the end of our discussion with Baroness Ashton we had an exchange about the secrecies surrounding the work of the Multi-Disciplinary Group on the Data Protection Framework Directive, which, of course, applies to the whole of the third pillar. Do you not think that if the public is to have confidence in the arrangements that are being developed we need to know more about what goes on in the MDG? Are you not personally anxious that the general data protection regimes which will apply to third pillar data are being developed without the knowledge of the public or any of the parliaments in the European Union?
Joan Ryan: Obviously that is an issue for DCA, so I cannot step into that. Across the board, and as I have said here, the UK Government is always pressing to ensure there is greater transparency.

Q608 ***Earl of Listowel:*** Given what you have been saying about the importance of us working together effectively, have you been watching the development of the Schengen evaluation teams carefully? It has been planned that they should be allowed to make visits without warning and there should be increasing co-operation using their data with the national authorities'. This was part of The Hague Programme but has not been acted upon yet. Will you be watching to see that is moved forward given the priority it seems to deserve from what you have been saying?
Joan Ryan: I certainly will be watching carefully, yes. Given appropriate examination of all measures and good scrutiny, we very much want SIS II to be a big success; it is very important that it is.
Chairman: Minister, thank you very much indeed for your helpful answers to our questions and again to your colleagues. As I think you know, you are the last witness on our list and it has been very nice to have seen you here again. I think it will be clear to you some of the concerns that are worrying this Committee and it will no doubt be reflected in our report. When you and your colleagues look at the transcript, if you think there is anything further that we ought to know, perhaps to allay those concerns, we would be very happy to receive further evidence from you. I should politely thank you for your written evidence in July but, as I say, if there is anything supplementary that seems to you that we need to allay our concerns then please feel free to let us have them. May I thank you very much indeed for coming today. I am sorry, we have kept you for quite a long time. It has been very helpful of you, and I wish you good luck.

Supplementary written evidence by the Home Office

HOUSE OF LORDS INQUIRY INTO THE SECOND GENERATION SCHENGEN INFORMATION SYSTEM (SIS II): FURTHER EVIDENCE

Further to the Committee hearing at which I gave evidence on the 29 November, you invited me to submit a note addressing a number of points which were raised. This letter covers the points raised during the hearing that I undertook to provide a note on and updates the Committee on SIS one4all.

At question 574 the Committee asked about the timing of the impact assessment on the management of the Central SIS II and whether the UK will have any input into this assessment. A draft joint declaration of the Commission, Council and European Parliament provides that, within two years of their entry into force, the Commission must present further legislative proposals which will allow operational management of the central SIS and parts of the communications infrastructure to be entrusted to an agency. The impact

assessment must be carried out before the legislative proposals are brought forward. This will be produced by the Commission, so the UK will not have direct input. Once legislative proposals are brought forward the UK will participate in negotiations in the normal manner.

At question 581 the Committee requested a note on the reason for the delay to introduction of "one-to-many" searches. The European Parliament raised concerns about certain aspects of the use of fingerprints for identification in the SIS II. The Commission therefore agreed to produce a report on the availability and readiness of the required technology, and to consult the European. Parliament on this report, in order that its concerns should be addressed. The Committee is correct that the technology to permit "one-to-many" searching is already in use, and the Government is content that this functionality should be introduced following the Commission's report. The draft Regulation and Decision establishing SIS II provide that the European Parliament should be consulted. It would be unable to block the introduction of the technology, but the Council will seek to ensure that its concerns are addressed as far as possible before the technology is introduced. The same would apply to any concerns raised by national governments or parliaments.

At question 591, the Committee requested more information on the future resource implications of SIS II for our operational partners. The SIS II business case includes operational costs for the Crown Prosecution Service (CPS), the Metropolitan Police Service (MPS) extradition team and Court Services. This is a work in progress and the process of agreeing changes in budgets will not be done until a full and robust assessment of the impact of SIS II upon the various operations involved has been carried out. The Home Office will work closely with SOCA, CPS, ACPO and ACPO(S), the MPS Extradition Unit, the Department for Constitutional Affairs and the Office for Criminal Justice Reform to determine the likely impacts on workload. Conclusions will be reached in the coming year.

In relation to question 593, the Committee asked for further details of costs to the taxpayer of SIS I. The Government estimates that the final cost of the SIS I programme before transition to SIS II was approximately £35 million. The main benefit derived so far is a staffed SIRENE bureau based in SOCA with an operational information management system currently used to deal with European Arrest Warrants although not connected to the SIS. This information management system has been extended to deal with SOCA's Interpol and Europol business.

Finally, I would also like to take this opportunity to update the Committee on the proposal for SISone4all. On 5th December, the JHA Council gave the go- ahead for SISone4all to proceed. Currently the UK has no intention to join SISone4all and we negotiated the terms of the Council Conclusions relating to financing the project so as to exempt the UK from future additional costs associated with implementing SISone4all.

I hope that this addresses the outstanding questions raised by the Committee.

14 December 2006

Memorandum by JUSTICE

Introduction

1. JUSTICE is an independent all-party law reform and human rights organisation, which aims to improve British justice through law reform and policy work, publications and training. It is the UK section of the International Commission of Jurists. JUSTICE has been strongly involved in monitoring the development of a European area of freedom, security and justice and seeks to ensure that individual rights are adequately protected in tandem with the development of efficient police and judicial co-operation in criminal matters. We have closely observed the development of the Schengen Information System and have published a report on the System in 2000 ("*The Schengen Information System—A human rights audit*").

2. We are grateful for the opportunity to submit written evidence on the development of the second generation Schengen Information System (SIS II), which we believe to be a development meriting detailed and comprehensive parliamentary scrutiny.

3. At the outset of our evidence we would like to point the Sub-Committee to the notorious difficulties for non-governmental organisations such as JUSTICE to obtain up-to-date information about the current state of Commission proposals for legal instruments, such as SIS II, under negotiation in the EU Council. These difficulties severely hamper the ability of these organisations to monitor effectively, and comment on, the legislative process under the Third Pillar. There is indeed a need for considerably greater transparency and timely accessibility of documents at Council level in order to achieve an acceptable level of accountability towards European citizens.

29 November 2006

4. In the course of our comments, we will confine ourselves to an analysis of the SIS II as envisaged by the EU Council in the current draft Regulation of the European Parliament and of the Council on the establishment, operation and use of the SIS II ("the Regulation"; based on Commission proposal COM(2005) 236 final) and the Council Decision on the operation on the establishment, operation and use of the SIS II ("the Decision"; based on Commission proposal COM(2005) 230 final). We will not comment on the third SIS II instrument, the Regulation giving access to SIS II data by vehicle registration authorities (COM(2005) 237 final).

Key Observations

5. JUSTICE is alive to the necessity to re-evaluate the SIS and improve its functioning in light of the need of new EU member states to participate in the system. Where border controls between member states are being abolished there is a clear need to compensate this openness by means of enhanced information exchange allowing for measures to be taken to protect the safety and security of all people living in the EU.

6. We are concerned, however, that the development and introduction of SIS II is not just being used to accommodate a greater number of member states participating in the system and technically improving the one currently in operation, but also to extend its scope and purpose beyond that of merely compensating for the abolition of border controls between member states. In the context of a growing desire of member states to improve information exchange between judicial, law enforcement and asylum and immigration authorities, the introduction of a new generation SIS should not be used to put in place an information exchange mechanism that goes beyond what is needed to compensate for the absence of border controls between member states. The trend towards a comprehensive information exchange architecture in Justice and Home Affairs (JHA) in the EU needs an open, informed and in-depth debate. The overhaul of the SIS is a good opportunity to engage in such a wider discussion; yet, this does not seem to be what the Commission and Council had in mind when embarking on the process of improving the SIS.

7. It is therefore JUSTICE's main concern that the development of SIS II is not limited to improving the day to day technical working of a border control data exchange mechanism but broadens its scope without adequate prior discussion of the consequences of the planned changes.

8. JUSTICE believes that the present Council drafts of the SIS II Decision and even more so the SIS II Regulation:

- may create considerable confusion as to their purpose and scope and thus; and
- may not sufficiently respect the principle of strict purpose limitation of personal data.

9. In respect of the grounds for SIS alerts and the general data protection regime in the Council drafts of both the Regulation and the Decision, we recognise that those drafts indeed contain certain improvements in relation to the SIS I provisions. However, these drafts also still show significant shortcomings and weaknesses. We particularly believe:

- that, on account of the current Pillar structure in EU law, the data protection regime governing the SIS II is too complex and confusing;
- that the grounds for issuing an alert under the Regulation leading to the refusal of entry into a member state of the affected person remain too vague and that no efforts have been made to harmonise those grounds for an alert;
- that third country nationals enjoying free movement rights will still be subject to Schengen alerts for immigration purposes;
- that data protection rules in the Regulation and Decision with regard to the exchange of supplementary information and national copies of the CS-SIS remain dissatisfactory and unclear; and
- that the information and data access rights of data subjects and the remedies against inaccurate information remain insufficient, with too much leeway given to member states to constrain information and data access rights through blanket references to member states' laws throughout the SIS instruments.

Interoperability, Purpose Limitation and Data Access Under the SIS II Instruments

10. JUSTICE's main concern with the draft Council instruments providing the legal basis for SIS II is the unclear scope and purpose of the proposed information system.

Interoperability and purpose limitation

11. Under the general data protection principle of strict purpose limitation of the use of personal data, the scope and purpose of a database has a significant bearing on the group of users who may lawfully access a database and process the data held on it. This principle commands that there be a strict nexus between the purpose of a data collection and the use that can be made of the data.

12. It is against the backdrop of the general discussion on the so-called interoperability of EU JHA databases that the concept of purpose limitation in the SIS II becomes a dominant issue. The Commission apparently considers interoperability of databases to be primarily a technical concept (see the Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among databases in the area of Justice and Home Affairs, 24 November 2005, COM(2005) 597 final).

13. We question this narrow understanding of the concept of interoperability. As the European Data Protection Supervisor in his opinion of 10 March 2006 has pointed out, technical interoperability will inevitably raise the issue of the granting of access of persons or agencies to databases to which they would not have been given access under a strict reading of the original purpose of the respective database. Interoperability in this wider sense is thus likely to involve a redefinition and, necessarily, a broadening of the purpose of a data collection. There would be no need to ensure technical interoperability were it not intended that there should also be interoperability in a legal sense of making lawful access to certain data collections beyond the initial purpose for which the data was collected. In this sense, interoperability might not, as such, conflict with the principle of purpose limitation, as the measure laying down the principle of interoperability would have the effect of changing the purpose limiting the use of the data concerned. However, such comprehensive interoperability of JHA databases could have the effect of rendering the principle of purpose limitation practically meaningless in limiting the access to, and use of, personal data in specific databases.

14. We therefore notice with concern the move at EU level towards general database interoperability and the establishment of a system of increased access to JHA databases for law enforcement purposes by security and criminal justice agencies in the broadest possible sense.

15. One example for this trend is the Commission proposal for a Council Decision concerning access for consultation of the VIS by the authorities of member states responsible for internal security and by Europol for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences (24 November 2005, COM(2005) 600 final) and, more generally, the aforementioned Commission Communication on interoperability of JHA databases of the same day. Both envisage the access by member states' internal security agencies to the VIS for the purpose of fighting terrorism and serious crime. The Communication also discusses granting law enforcement agencies access to SIS II and EURODAC for the same purpose. Defining the legal limit for access by law enforcement agencies, the Commission proposes to use the definitions of terrorism and serious offences as laid down in the Council Framework Decision 2002/475/JHA on combating terrorism and the Europol Convention and its annex respectively. While these proposals are thus limited in their scope to serious threats to public life,[1] member states seem to push for more than that, intent on granting access to all three JHA databases for wider law enforcement purposes not limited to the most serious forms of criminality.

Who will get access to SIS II?

16. The SIS II Regulation and Decision exemplify this desire of member states to extend access rights to the SIS II database to authorities beyond those involved in external border control or checks in lieu of intra-Schengen border controls. Arts 17(2) and 37(2) of the current Council drafts for the Regulation and Decision, respectively, provide for access to SIS II data for "national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation". This provision, which was not included in the original Commission proposal, takes SIS II access rights under the Regulation outside the context of

[1] Unavailability of these documents does not allow JUSTICE to verify if this test has been retained in the current Council drafts of the VIS access proposal or whether member states are negotiating a lower threshold in line with the current SIS II Council drafts.

border controls and the compensation for the abolition thereof between the Schengen states, and gives certain authorities involved in the national criminal justice systems the rights to access SIS II immigration data (or, under the Decision, to SIS II data relating to alerts for surrender under the EAW scheme etc). Access will not be limited to terrorism offences or other serious forms of criminality.

17. Furthermore, these provisions leave open the question, who these national judicial authorities with SIS II access rights could be, as they are not defined in the Council drafts. As prosecuting authorities take responsibility for the initiation of criminal prosecutions in most member states, it is obvious that they, and not just courts, will qualify as "judicial authority" within the meaning of arts 17(2) and 37(2). It is far from certain, whether the wording of these provisions would exclude police forces from the circle of those being granted access to SIS II data under the Regulation and Decision. With some imagination, arts 17(2) and 37(2) could be read as including at least certain forms of police forces mandated by prosecuting authorities to carry out investigations for breaches of the criminal law.

18. Obviously, the SIS in respect of alerts on persons and objects for discreet checks—even in its current, first generation version under Art 99 CISA—has, by its very nature, a certain investigative function. However, we think the third-country nationals' part of the current SIS I+ does not. Art 101 CISA does not grant law enforcement authorities access to data held on the SIS. The inclusion of (judicial) law enforcement authorities into the circle of those having routine access to SIS II data may therefore be the starting point for a transformation of SIS II (and particularly its First Pillar part) into a veritable investigative tool for general crime detection and investigation purposes. Similarly, the provisions on interlinking of alerts (art 26 Regulations, art 46 Decision), particularly where combined with the law enforcement authorities' access rights envisaged in arts 17(2) and 37(2) of the Council drafts, will further steer SIS II towards becoming a fully fledged general purpose law enforcement database, rather than one limited to the purpose of being a compensatory measure for the abolition of border controls between member states, as envisaged in recital 5 of the current Council draft Regulation.

19. This wider purpose of the SIS II, consonant with the trend towards technical interoperability and provision of more general law enforcement database access rights, may conflict with the principle of purpose limitation in light of the rather narrow scope of legal bases of the SIS II as laid down in arts 2(1) of both the Regulation and Decision. This narrow core purpose of the SIS II—at least its immigration part under the Regulation—is also reflected in art 21(2) of the draft Regulation, where it states that "[t]he member states may process the data provided for in Article 15 for the purposes of refusing entry or stay in their territories." It remains unclear whether this provision indicates a strict purpose limitation for SIS II immigration data (in the sense of "may ONLY process . . ") or whether it does not have any specific meaning in the context of purpose limitation at all. The wide access rights afforded to judicial authorities under art 17(2) of the Regulation would militate in favour of the latter interpretation. Further clarification of the relationship between arts 17(2) and 21(2) of the Regulation is certainly needed.

20. We wholeheartedly endorse the poignant remarks in the opinion of the Schengen Joint Supervisory Authority (JSA) of 27 September 2005. JUSTICE's concerns about the adherence of SIS II to the principle of purpose limitation are exemplified not only by art 17(2) of the draft Regulation, but also more generally by the failure to include in the Council drafts a provision which was originally contained in the Commission proposals for the said instruments and which reiterated the importance of the purpose limitation principle for processing and accessing the data held on the SIS II. Arts 16(2) of the Regulation and 39(2) of the Decision as originally envisaged by the Commission provided that "[t]he data referred to in paragraph 1 shall only be used to identify a person for the purposes set out in this Regulation/for the purpose of identifying a person in view of a specific action to be taken in accordance with this Decision." We are disappointed to find this provision removed from the current Council drafts.

21. The Commission's and Council's desire to achieve technical (and legal) interoperability between EU databases, the discrepancy between the "general objective" of the SIS II and the "scope" of the SIS II legal instruments as amply expressed through the widening of access rights especially for immigration data held under the SIS II Regulation, demonstrate the urgent need for a comprehensive discussion at member states' and EU level of the way information exchange in Justice and Home Affairs should be organised and regulated. This inquiry may prove to be a motor for such a discussion.

The Legal Framework for the Operation of the CS-SIS

22. On the issue of the management of the central SIS II (CS-SIS) by the Commission and, in due course, by the Management Authority envisaged in the SIS II legal instruments, and its legal accountability, JUSTICE embraces the position adopted by the Schengen JSA in its opinion of 27 September 2005. It does not need repetition here.

23. We would like to point out, though, that the legal data protection regime governing the data processing by the Management Authority does not seem to be sufficiently clear (this is a criticism that applies to the data protection regime and the EU pillar structure in general and is elaborated below under marginal note 38). While those aspects of the work governed by the SIS II Regulation will be covered by that instrument as *lex specialis* and the Regulation (EC) 45/2001 of the Parliament and the Council on the protection of individuals with regard to the processing of personal data by Community institutions and bodies as subsidiary *lex generalis*, no such *lex generalis* at EU level exists for the Third Pillar data processing by the CS-SIS II under the SIS II Decision.

24. The original Commission proposal for the Decision, in recital 21, contained a clarification to the effect that data processing by the Commission (or Management Authority) would also be governed by the Regulation EC 45/2001 mentioned above; however, the proposal did not contain a proper provision to that effect. Without entering the debate on the legal effect of a decision recital, we have to state that we do not have knowledge of whether or not this recital has been retained in the current Council draft of the Decision. Even if this were to be the case, the inclusion of an express provision in the body of the Decision, unambiguously declaring the applicability of the said Regulation, would be called for to ensure applicability of that instrument.

25. The prospective Third Pillar Data Protection Framework Decision would not, as such, apply to the Management Authority since this type of legal instrument cannot be addressed to EU bodies; a further, specific Council Decision would thus be needed to extend the scope of the Framework Decision to EU bodies. Currently, art 49 of the draft SIS II Decision declares that personal data shall be protected in accordance with the amended Council of Europe Convention No 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. While this Convention provides a minimum basis for data protection, we consider it indispensable that a comprehensive subsidiary data protection regime at EU level is in place to govern the work of the CS-SIS II Management Authority.

Criteria for Schengen Alerts Under the SIS II Regulation

26. JUSTICE is disappointed that the chance for harmonising the criteria leading to the issuing of a Schengen alert on refusal of entry or stay of third country nationals under art 15 of the current Council draft of the Regulation may be lost.

27. Alerts under art 15 of the Regulation (the former "art 96 alerts") represent by far the largest number of all alerts on the present SIS. As the "Report of the Schengen JSA on an inspection of the use of Article 96 alerts in the Schengen Information System" of 20 June 2005 demonstrates, there is an unacceptable divergence of national practices on the issuing of said alerts. In some member states expulsion decisions lead automatically to an SIS alert; in others a separate decision (and thus a separate verification of the necessity of an SIS alert) is needed. Two member states are notorious for issuing alerts for all failed asylum seekers, other member states do not operate such an automatic alert policy. Endorsing the Schengen JSA's recommendation in its report, JUSTICE considers it imperative that the criteria for art 15 alerts be harmonised so that a higher degree of uniformity and consistency of art 15 alert decisions across the EU can be achieved.

28. While art 15(3c) of the current Council draft of the Regulation now provides for a review of the conditions for issuing alerts three years after SIS II becomes operative and allows the Commission to make proposals for a modification of these conditions "to achieve a higher level of harmonisation", the stricter conditions for an alert proposed by the Commission in its original draft have not been adopted by the Council. Consequently, recital 10 of the Regulation as proposed by the Commission, stating that "it is appropriate to further harmonise the provisions on the grounds for issuing alerts" and that "the grounds for issuing such alerts [. . .] should be more homogenous", has been deleted in the Council negotiations.

29. Regrettably, art 15 of the present Council draft of the Regulation does not lay down more specific grounds for issuing an alert than its precursor, art 96 CISA. Moreover, it appears that some criteria for the issuing of an alert have indeed been relaxed in the current Council draft in the sense that the evidentiary threshold for the issuing of an alert on grounds of a perceived threat to public policy or public security seems to have been

lowered: while in art 96(2)(b) CISA the threshold was the existence of "genuine evidence of the intention to commit [. . .] offences", in the current Council draft the test now is the lower one of "clear indications of an intention to commit such offences". The original Commission proposal for the SIS II Regulation did not even contain a criterion along the lines of art 96(2)(b) CISA or art 15(2)(b) of the Council draft at all. We consider the evidentiary threshold in art 15(2)(b) of the draft Regulation as unnecessarily low and altogether too vague.

30. Similarly, the alert criterion of a conviction of a third country national under art 15(2)(a) of the Regulation (the former art 96(2)(a) CISA) remains unnecessarily restrictive; a chance to achieve at least a very basic harmonisation of this criterion along the lines of the original Commission proposal is being foregone. The Commission proposal envisaged an alert for a criminal conviction only in cases where the offence was one contained in the list in art 2(2) of the Council Framework Decision 2002/548/JHA on the European Arrest Warrant; furthermore, the penalty following the conviction would have had to be one "involving deprivation of liberty of at least one year". The current Council draft does not follow this suggestion but rather reverts to the formulation contained in art 96(2)(a) CISA, mandating an alert for a conviction for "an offence carrying a penalty involving deprivation of liberty of at least one year". It seems to us that one subtle, yet significant difference between the Commission proposal and the Council draft is the formulation of the one-year-sentence condition: where a third country national is convicted of an offence carrying a minimum one year custodial sentence but is then given a suspended custodial sentence, it is doubtful whether this sentence would amount to a penalty involving deprivation of liberty within the meaning of the Commission proposal. Conversely, a suspended custodial sentence where the offence carries a sentence of at least one year imprisonment would certainly fulfil the condition for an alert under the current Council draft. JUSTICE believes that the presence or stay in the member state of a third country national whose custodial sentence has been suspended by the sentencing judge cannot, as a rule, be considered a threat to public policy or public security. An alert should therefore not be issued in respect of such a person. While we find it difficult to assess, in full detail, the consequences of the difference in the formulation of the test discussed now, we consider the more narrow Commission formulation of art 15(2)(a) of the Regulation to be preferable for reasons of legal certainty.

31. JUSTICE regrets that neither the Commission nor the Council seem to have made any efforts to tackle the issue of the near automatic SIS alerts for failed asylum seekers in two of the member states. We consider it highly desirable that uniform rules as to the treatment of failed asylum seekers as regards SIS alerts be put in place.

32. We acknowledge, however, the potentially beneficial effect of the proportionality clause for the entry of an alert contained in art 14B of the Council draft. It remains to be seen, though, whether national authorities and courts will give meaning to this clause by applying it robustly in the course of the daily operation of the SIS II.

33. The somewhat unclear effect of the individual assessment clause in art 15(1) of the Regulation on the conditions for the issuing of an alert will be addressed in the following paragraphs.

The Inclusion of Third Country Nationals Enjoying Community Free Movement Rights

34. The current Council draft of the Regulation contains, in art 15A, a rather awkwardly formulated provision, laying down that art 15 alerts concerning third country nationals enjoying Community free movement rights shall be made in conformity with rules adopted in implementing the Free Movement Directive 2004/38/EC of 29 April 2004. In art 15(1) of the Regulation, it is also decreed that an alert decision "may only be taken on the basis of an individual assessment".

35. JUSTICE welcomes the inclusion in the draft Regulation of these provisions. They should ensure application of art 15(2) of the Regulation in conformity with the free movement restriction provision for third country nationals contained in art 27(2) of the Free Movement Directive. We think, however, more unambiguous guidance as to the treatment of third country nationals enjoying Community freedom of movement could, and indeed should, be provided in the SIS II Regulation itself. This could be done by incorporating into art 15 or 15A of the Regulation a provision mirroring the said art 27(2) of the Free Movement Directive in light of the ECJ's recent judgment in *Commission v Spain* (C-503/03; 31 January 2006, see below marginal note 38).

36. Such clearer guidance might add more weight to the individual assessment clause now contained in art 15(1) of the Regulation. Generally, though, we remain somewhat puzzled as to the precise effect of the individual assessment clause: while art 15(1) exhorts the member states to carry out an individual assessment as to whether the concerned person's presence in the member state poses a threat to public policy or security, art 15(2) provides in effect that such a threat is to be presumed where the conditions of art 15(2)(a) or (b) are

fulfilled. We would thus consider the individual assessment clause to act as an emergency brake in cases where contra-indications to the presumption effectively laid down in art 15(2)(a) and (b) are present and would militate against a finding of a person's presence being a security threat.

37. Generally, however, JUSTICE would prefer a complete ban on SIS alerts for third country nationals enjoying Community free movement rights. Such a ban and corresponding duty to erase existing alerts upon the acquisition of free movement rights under EU law could be modelled on art 20 AA of the current Council draft. We cannot see the need to treat differently EU citizens (for whom an SIS alert cannot be issued) and third country nationals with free movement rights (who will typically be spouses or close family members of an EU citizen) when it comes to SIS alerts. Both categories of persons can be refused entry under art 27(2) of the Free Movement Directive; thus it smacks of an unjustifiable discrimination to allow SIS alerts for one category of free movement rights holders, but not for the other.

38. With regard to the ECJ's recent seminal judgment in *Commission v Spain* (C-503/03), we consider that it is the new Schengen Borders Code (Regulation (EC) No 562/2006 of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders, coming into effect on 13 October 2006) that will be affected by the Court's decision. While we do not believe that the continued inclusion of third-country nationals with free movement rights on the "immigration SIS II" is called for, we consider the current draft to be in compliance with the ECJ's ruling in *Commission v Spain*. It was the SIS-specific automatism of a refusal of entry as a consequence of an art 15 alert under art 11(1) in conjunction with art 5(1)(d) of the Schengen Borders Code (the present art 5(d) CISA) that the Court was most critical of in its decision and not the holding of data of this category of persons on the SIS. While the Schengen Borders Code is not, as such, the subject of the present inquiry, we think it important not only to consider the conditions for an SIS II alert under art 15 of the Regulation, but also the consequences of such an alert, some of which are laid down by the Borders Code.

Data Protection Considerations

A confusing legal regime under the pillar structure

39. What makes an analysis of the data protection regime governing the SIS II a rather complex if not cumbersome exercise is the fact that the SIS II will be governed by a confusing number of legal instruments on data protection. This is due to two reasons: first, the distribution of lex specialis data protection provisions between the different SIS II instruments (the Regulations and the Decision) and the subsidiary leges generales contained in the EC Data Protection Directive 1995/46/EC governing data processing by the member states, the Regulation (EC) No 2001/145 governing data processing by Community bodies, the Council of Europe Data Protection Convention No 108 of 28 January 1981 and a prospective Third Pillar Data Protection Framework Decision. Secondly, this proliferation of data protection instruments has its cause in the increasingly anachronistic pillar structure of the EU, which the failed constitutional treaty would have ended. Thus, the SIS II Regulations, as First Pillar instruments, are subject to the subsidiary First Pillar data protection directives and regulations, whereas the SIS II Decision, as a Third Pillar instrument, will provisionally be governed by the Council of Europe Data Protection Convention (as envisaged in art 49 of the draft Decision) and, subsequently, by a Third Pillar data protection instrument.

40. JUSTICE believes that this distribution of data protection provisions over numerous instruments may create a risk of uncertainty for everyone involved in the practical application of data protection provisions to data processing in the context of the SIS II. It can also lead to a curious divergence of data protection standards between the different instruments.

41. One example of such a divergence of standards are the provisions in the current Council drafts governing the transfer of data to third countries. While art 48 of the Regulation would not allow to make available or transfer the data processed under the SIS II Decisions (Third Pillar), data processed under the First Pillar SIS II Regulation would be subject to transfer to third countries under the conditions laid down in the EC Data Protection Directive and the Community Data Protection Regulations. These instruments do not contain a blanket ban on transfer of data held on the SIS II to a third state. We cannot see a reason for this difference in treatment.

42. While we would reiterate our urgent call for the adoption and implementation of a robust Third Pillar Data Protection Framework Decision, we would like to see the creation of a uniform data protection regime for all data processing on the SIS II irrespective of the pillar under which data is being processed.

Biometric data

43. JUSTICE shares the concern voiced, inter alia, by the EDPS and the Schengen JSA, about extensive reliance on biometric data (photographs and fingerprints) on the SIS II as primary identifiers.

44. We therefore notice with approval the inclusion of special rules for biometric data in arts 14 C and 14 AC of the Council drafts of both the Regulation and Decision, especially the rules on special quality checks of biometric data. We hope that these quality check rules will allow a thorough verification of the accuracy of data, bearing in mind the potential use of fingerprints as identifiers for SIS II purposes under arts 14 C(c) and 14 AC(c) of the current Council drafts. We also most warmly welcome the two-year review clause of the use of the biometrics functionality in arts 14 C(d) and 14 AC(d). We expect this review also to cover any practical problems that might have arisen from the use of biometric data in the context of SIS II.

The rules governing supplementary information

45. We regret that the current drafts of the SIS II instruments only inadequately regulate the provision and exchange of so-called supplementary information. According to the definition provided in arts 3(1)(b) of both the draft Regulation and Decision, this is information which is not held on the SIS II and will be made available in a number of situations enumerated in the said provisions.

46. These situations in which additional information may be exchanged are only defined in the most vague and open-ended terms in art 3(1)(b). Pursuant to arts 8 of the draft SIS II instruments, details of the exchange of supplementary information and the nature of such data will be regulated by the SIRENE Manual, as adopted under the comitology procedure provided for in arts 35(3) of the Regulation and 61 of the Decision. No guidance as to the exercise of this rulemaking power is contained in the SIS II instruments themselves. Supplementary information may comprise highly sensitive personal data, we therefore believe that laying down rules for the exchange of this information should not be left to the member states acting under the comitology procedure, but regulated in greater detail in the main legal instruments providing the basis for SIS II. To regulate only the conversation periods of such supplementary information in the primary instruments (as under arts 27 of the Regulation and 47 of the Decision) has to be regarded as insufficient.

Data accuracy and quality

47. JUSTICE is disappointed to notice that the provision in art 24(7) of the Commission's original draft Regulation, requiring member states to review data held on the SIS at least annually, has been removed in favour of a simple duty of member states to ensure that data is accurate (arts 24(1) of the Regulation and 43(1) of the Decision). We believe that strict, harmonised review periods are an essential and indispensable element for a fair operation of a system such as SIS II, as inaccurate data increases the risk of unjustifiable decisions being taken by member states' authorities.

National copies

48. Issues of data accuracy arise particularly in respect of national copies of the data held on the CS-SIS II. While the central system will ideally contain an accurate set of data, updated, when necessary, by the relevant member state, use of national copies may increase the risk of relying on, and operating with, outdated and thus inaccurate data. We therefore regret the deletion from the original Commission draft of the SIS II instruments the duty of member states to ensure that the national copies are at all times identical and consistent with the CS-SIS (arts 9(2) of both the Regulation and Decision). The new arts 9(2) only speak of equivalent results which searches in the national copy and the CS-SIS have to yield.

Interlinking of alerts

49. We appreciate the fact that links between alerts as provided for in arts 26 of the draft Regulation and 46 of the draft Decision must not have the effect of widening law access rights and may only occur where there is a clear operational need. However, we are not convinced that an interlinking of alerts, being essentially an investigative tool, will sit easily with the principle of purpose limitation of the data held on the SIS II. On the (contested) assumption that SIS II—certainly its immigration part under the Regulation—should not have the

function of a tool for general crime investigation purposes, it is difficult to justify the creation of links between SIS immigration data under the Regulation and those of a more law enforcement oriented type under the SIS II Decision. The need to link alerts should thus be very carefully examined.

Data transfer to third countries

50. While there may be situations calling for a transfer of personal data held on the SIS II to third countries, JUSTICE is surprised at the differential treatment in this respect of immigration data (which will be subject to the third country data transfer provisions of the EC Data Protection Directive) and other SIS data, for which the draft Decision contains a bar on transfer to third countries (art 48). We would urge the Sub-Committee for an explanation for this difference in treatment.

Rights of the Data Subject

51. Adequate information and access rights and meaningful legal remedies are a crucial element of an information system, under which alerts can have automatic and harsh consequences, such as the refusal of entry into an EU member state of third country nationals under the Schengen Borders Code.

52. We generally welcome the level of rights accorded the data subject in the current Council drafts of the SIS II instruments. However, we believe that the rights and remedies provided for in the current drafts could be improved, making them more effective for the data subject. In particular, we are of the view, that the role of member states' national law in determining the extent, exceptions and implementation of those rights and remedies is a too wide-ranging one. A higher degree of approximation or even harmonisation of these safeguards for a fair functioning of the Schengen system is called for.

Right of information

53. While a right of information of the data subject about the data being held on him or her by the data controller exists for third country nationals under art 29 of the draft Regulation in conjunction with arts 10 and 11 of the EC Data Protection Directive, no such right of information is provided for in the draft SIS II Decision for Third Pillar data. While it has to be acknowledged that the latter category of data may be of a more sensitive nature than immigration data held on the SIS, a right of information with a general national security/safety exception (as in art 29 of the draft Regulation) could and should be provided for without compromising the sensitive nature of the data where this would be an issue.

54. With regard to the exceptions to the right of information of third country nationals contained in art 29(a)–(c) of the SIS II Regulation, we are concerned about the blanket nature of the reference to national law under art 29(c). While the provision lists examples of circumstances in which member states' laws could restrict the information right, this list is only indicative (". . . in particular in order to safeguard national security, defence, public security" etc). Thus this provision leaves member states free rein to limit the right of information as they please with no meaningful judicial oversight by the ECJ. Restrictive national legislation may even lead to the risk that this important right will be little more than an empty shell in practice.

55. The Commission proposal, however, did not contain such a reference to national laws. We would urge the Sub-Committee generally to take a strong line on the extent to which the current SIS II Council drafts rely on member states' domestic laws when fleshing out (or rather limiting) the data protection standards and the rights a data subject has to enjoy throughout the EU. Bearing in mind the differences in domestic data protection standards between EU member states in the area covered by the Third Pillar, the establishment of meaningful and robust data protection standards across the EU depends on the level of harmonisation (or at least significant approximation) of member states' laws in this area. Such harmonisation cannot be achieved by blanket references to member states' laws where limitations of the rights of the data subject are concerned.

56. We also consider the data subject's right of information not to be strong enough. As we have already highlighted in our publication on SIS I in 1999, not only should a data subject be furnished with information that data on him or her is held on the SIS II (and perhaps even what kind of data are stored), but also he or she should be provided with standard information about his or her legal remedies. Art 28(e) of the current SIS II draft Regulation does not go that far. We believe that legal remedies, such as those provided for in arts 30 of the draft Regulation and 52 of the draft Decision, are only effective where they are practically accessible,

in particular, where the individual entitled to the remedy is made aware of its existence and the procedure for claiming it correctly. It would be desirable to devise a standard "letter of rights" for data subjects, which would explain the legal remedies available to them in a language they can understand.

Right of access, correction and deletion of data

57. JUSTICE is concerned that the formulation of the provisions governing the data subject's right of access to the personal data held on the SIS II (arts 28 of the Regulation and 50 of the Decision), once again, leaves too much leeway for national laws to undermine the general right of access enshrined in these provisions. It remains unclear how far the substantive right of access under art 28 and 50 of the SIS II instruments reaches and to what extent member states may lawfully make inroads into this general entitlement when regulating the way in which the right of access to the SIS data may be exercised. Harmonisation of domestic data protection standards at a high level can hardly be achieved where there is only insufficient guidance as to the implementation and enforcement of the abstract right of access to one's personal data.

58. Similarly, the exception to the general rule on access to data contained in arts 28(2) and 50(s) of the current Council drafts attracts concern: according to these provisions, which did not form part of the original Commission proposals, "communication of information to the data subject shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedom of others." The first alternative of the test for the lawfulness of a member state's denial of access to information held on the SIS II appears overly broad and deviates in this aspect significantly from the model provided for in art 13 of the EC Data Protection Directive: according to arts 28(2) and 50(2) access to data may be refused where this would be indispensable for the performance of any lawful task of member states' law enforcement agencies.

59. The provisions do not distinguish between lawful tasks of law enforcement agencies of different importance and thus do not contain a balancing requirement obliging member states to weigh the infringement of the data subject's right of access to the SIS data against the likely effects of access to data on the criminal justice system and crime detection and investigation. Denial of access to the SIS data cannot be considered proportionate in cases where the police or public prosecutors are performing a lawful, albeit quite insignificant, task and where only a denial of access to the SIS II data would ensure that that task was fulfilled. Without engaging in a balancing exercise and robustly applying the proportionality test, denial of access to a data subject's SIS data may amount to a violation of the concerned individual's right under art 8 ECHR.

August 2006

Printed in the United Kingdom by The Stationery Office Limited
3/2007 357850 18595