University of Sussex
Sussex Centre for Migration Research

The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU?

Sussex Migration Working Paper no. 30

Alice Garside

March 2006

Abstract

The abolition of internal borders in the EU has enabled greater free movement, a privilege now taken for granted by EU citizens. It also created the momentum to find alternative means to ensure that the EU remains an area of freedom, security and justice. With people ever more mobile, the collection and sharing of data regarding the security risks presented by this migration has become an attractive, if expensive, option. The Schengen Information System is the largest database in Europe in the spheres of migration and cross border judicial and police cooperation, and is used to process personal information for the purposes of excluding individuals from the EU. Many of the important details and political choices behind the system's development are obscured by an opaque decision making process and the absence of important secondary legislation. The proposed changes to this system bring significant risks and uncertain opportunities and introduce, by stealth, the data surveillance of EU nationals.

Introduction

The Schengen Information System ("SIS") is an EU-wide database of persons and objects whose presence in or entry to the Schengen area[1] of Europe raises issues of public order or security. It became operational on 26 March 1995 and was created as a counterbalance to the suspension of border controls within the Schengen area. All EU member states plus Iceland and Norway[2] have access to the SIS, with the exception of the UK and Ireland who do not currently participate.

The information on the SIS includes data on persons wanted for arrest for extradition (Article 95), persons refused or to be refused entry to the Schengen area (Article 96), missing persons or persons who need to be placed under protection (Article 97), persons sought by judicial authorities in connection with criminal proceedings (Article 98) or objects or persons who are to be the subject of discreet surveillance or a specific check (Article 99). It contains the details of 818 673[3] people, 87 % of which have been recorded on the system under Article 96 for the purposes of refusing them entry to the Schengen area.

The SIS gives end-users such as police, border and customs agencies at frontiers and within the country[4] an instant search procedure to access information entered in the system by agencies in other states implementing the Schengen Convention [5].

The present system bears some amendments from the SIS when it came on line. Rising preoccupation with the impact of terrorism on public security also led Spain to propose new anti-terror functions for the SIS[6], many of which have now come into force. These measures, the SIS+1, include the grant of wider access to judicial and law enforcement agencies, and the inclusion of information on residence documents.

The limitations of the present system cannot cope with EU enlargement and the increased access to the system and incorporation of information provided by acceding states and "technical" measures were proposed to create the SIS II. The SIS II will include the addition of new categories of alerts and fields, the interlinking of alerts, the modification of the duration of the alerts, and the processing of biometric data[7]. It "will provide the technical flexibility" to expand its "functionalities" [8]. The Commission has now put forward proposals for the SIS II including a Parliament and Council regulation on immigration issues and a Council decision on police and criminal matters[9] (the "Proposed Regulation and Decision"). These measures will replace Articles 92 - 119 of the Schengen Convention. The new system is to be adopted by the end of 2006[10] and should come into operation in the first semester of 2007[11] once the information contained in SIS is migrated to the SIS II.

The principal rules of data protection and the right to privacy applicable to the SIS and SIS II are those contained in the Schengen Convention, the Convention for the Protections of Individuals with regard to Automatic Processing of Personal

---

[1] At present Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain and Sweden participate in the Schengen initiatives concerning the free movement of persons across internal borders.

[2] Council Decision 1999/437/CE OJ L 176, 10/07/1999 P. 0031 - 0033

[3] Note from Presidency on SIS Database Statistics, Doc No 8621/05, 2.6.2005

[4] Article 101 Schengen Convention

[5] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders Official Journal L 239 , 22/09/2000 P. 0019 - 0062

[6] Council Decision 2005/211/JHA and Council Regulation (EC) 871/2004

[7] Council Conclusions JHA of 5/6.6.3 re SIS docs 10054/03; 10055/03; 5003/2003 WG

[8] Commission Communication to the Council and EU Parliament COM (2003) 771 final Development of the SIS II and possible synergies with a future Visa Information System (VIS), p 15

[9] Proposal for Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II) COM (2005) 230 Final 31.5.2005 Council Doc. 9942/05 and Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) COM (2005) 236 Final 31.5.2005 Council Doc.9943/05

[10] Note from Presidency on JHA Council Declaration: follow up, Council Doc 11330/05, p5

[11] Note from Presidency on Parameters, procedures and time schedule for decision on the strategic management of SIS II, Council Doc 12888/04, 4.10.2004, p3

Data[12] ("Convention 108"), Directive 95/46/EC[13], Regulation (EC) 45/2001[14], and the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"). There is an emerging consensus Directive 95/46/EC's principles on data quality and availability should provide the foundations for all data protection in the EU, despite its purported non application to matters outside Community law.[15]. It represents a benchmark for data protection : adequate, specific, necessary to a specific legitimate objective and proportionate to the goal to be achieved.

Purpose

The SIS is a compensatory measure, whereby measures to facilitate infra community migration entailed the enactment of provisions to inhibit undesirable migration. There is a dark side of free movement where immigration control is a platform, a consensus builder, which brings with it a risk for the respect of privacy and adequate management of personal data.

Article 96 of the Schengen Convention, the focus of this paper, provides for data relating to aliens to be reported on the SIS for the purposes of refusing them entry to the Schengen area if their presence may pose a threat to public order or national security and safety. The article gives examples of such undesirables: those convicted of a criminal offence carrying a custodial sentence of one year or more, aliens for whom there are serious grounds to believe they have committed a serious offence, or genuine evidence that they intend to commit such an offence, or if the alien has failed to comply with immigration regulation or deportation measures.

The Proposed Regulation is different to Article 96 in that the threat posed by the presence of the third country national must be a *serious* one[16]. It also reiterates that a refusal of entry can be based on the threat posed to public policy. Public policy is broader than the exceptions of public order, national security or public safety allowed under Convention 108[17] Directive 95/46/EC[18]. The public policy motive for exclusion is a derogation from the fundamental principle of freedom of movement which must be interpreted strictly. The Proposed Regulation's Article 15 nonetheless improves on its predecessor in that the third country national must have been *sentenced* to at least a year of deprivation of liberty, and the measures purport not to apply to persons with EC rights.

From informational assistance to executive action.

Should information entered under Article 96 lead to refusal of entry or removal from the Schengen area, without the member state on whose territory the individual is seeking to enter or remain investigating the actual risk to public safety in their national territory, the existence of an alert rather than the risk posed by the individual becomes the basis for refusal of entry or deportation. This transforms the SIS from informational assistance to a freestanding cause for executive action. Such unquestioning reliance would be contradictory to the Recommendation of the European Council's Committee of Ministers regulating the use of personal data in the police sector which states that "As far as possible, quality of data should be verified at the latest at the time of communication (…) [and] judicial decisions, as well as decisions not to prosecute and data based on opinions or personal assessments checked at source before being communicated"[19]. No such checking exercise is built into the SIS's operation.

The SIS is managed through the SIRENE (Supplementary Information Request at the National Entry) bureaux network in different member states. The SIRENE bureaux are not responsible for verifying the accuracy of the data but for ensuring that data contained in different parts of the SIS is identical and aligned with the purpose of the Schengen Convention. The member state entering the information on the system is responsible for keeping the information up-to-date and accurate[20], yet a different member state may be taking action as a result of that information. The lack of procedural measures to verify SIS information before taking action

[12] European Treaty Series 108 - Automatic Processing of Personal Data, 28.1.1981

[13] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24.10.1995 *Official Journal L 281 , 23/11/1995 P. 0031 - 0050*

[14] Regulation (EC) 45/2001 of the European Parliament and of the Council OJ L 008, 12.1.2001 P 0001 - 0022

[15] Hustinx, Peter J. (2004), Speech by European Data Protection Supervisor, Budapest 1.12.2004, p2

[16] Article 15 (1) a

[17] Article 9

[18] Article 13

[19] Principle 5.5.ii Recommendation No. R(87) 15, adopted by the Committee of Ministers on 17.9.1987

[20] Article 105 Schengen Convention

undermines the system's ability to function lawfully as an instrument for executive action.

Investigative action and the merging of purposes

Against this creeping functionality lies a degree of protection. Article 102 of the Schengen convention provides that "Contracting Parties may use the data provided for in Articles 95 to 100 only for the purposes laid down for each type of report referred to in those Articles" [21] unless it is justified by the need to prevent an imminent serious threat to public order and safety, state security, or for the purposes of preventing a serious offence. No such guarantee exists in the SIS II, where links between Article 96 and other alerts are permitted under the Proposed Regulation[22] and Decision[23]. The details of how these links operate are not included in the proposed legislation – the Commission did not want to inflict the details on us : aspects such as the compatibility and links between alerts "cannot be covered exhaustively by the provisions of this Regulation due to their technical nature, level of detail and need for regular update"[24]. The answers are hidden in Council deliberations which clearly anticipate that Article 96 alerts would be linked to all other categories of alert[25]. The Council has provided some illuminating examples of these possible links: "96-98 - persons to be refused entry + witness in an illegal immigration case", "96-99pd - husband convicted criminal to be refused entry + wife suspected terrorist" or indeed "95-99 – husband wanted terrorist and wife suspected accomplice"[26].

Whereas the old SIS created a presumption, that data would only be processed in order to achieve the objective of the specific provision that warranted its entry on the system[27], the Proposed Regulation has a much wider vision whereby the purpose of the SIS II is to "enable competent authorities of the Member States to cooperate by exchanging information for the purposes of controls on persons or objects"[28]. The Commission offers little by way of precision : "data entered on the SIS II pursuant to this Regulation shall only be processed for the purposes and by the competent national authorities defined by the Member States in accordance with this Regulation"[29]. The Commission's explanation of the new functionalities is dangerously circular: "the list of SIS II functionalities contains the existing and the potential new functionalities"[30]. The purpose has become any purposes attributed to competent national authorities for the control of persons - a definition so wide as to create no certainty as to the purpose of the SIS II in practice.

Convention 108, Directive 95/46/EC and Regulation (EC) 45/2001 contain limitations on the purposes for which personal data can be stored. These provisions will apply to the SIS II regardless of the amendments contained in the Draft Regulation and Decision. Despite the attempt by the Commission in its proposed legislation to remove this restriction, certain overarching obligations should continue to apply. Saas points to the possible influence of the ECHR over national courts[31], but a challenge to the interlinking of alerts has yet to be made, as has a challenge before the European Court of Human Rights under Article 8 of the ECHR to the proportionality of refusing a visa or residence permit because of a registration on the SIS.

The President of the Council has acknowledged the transformation of the SIS : "the idea of using the SIS data for other purposes than those initially foreseen, and especially for police information purposes in a broad sense, is now widely agreed upon and even follows from the Council conclusions after the events of 11 September 2001"[32]. This represents the SIS II's development from a hit/no hit system into a much more complex, investigative instrument. The Schengen Joint Supervisory Authority ("Schengen JSA") who together with the European Data Protection Supervisor is is the European body currently responsible for monitoring the SIS and its successors' compliance with data protection

[21] Article 102 (3)

[22] Article 26

[23] Article 46

[24] Recital #19, Proposed Regulation

[25] Note from Presidency on SIS II functions/open issues, Council Doc No 12573/3/04, 30.11.2004, p3

[26] Note from Presidency on SIS II functions/open issues, Council Doc No 12573/3/04, 30.11.2004, p3

[27] Convention 108, Directive 95/46/EC and Regulation (EC) 45/2001

[28] Articles 1(1) Proposed Regulation and Decision

[29] Article 21 (1) Proposed Regulation

[30] Commission Communication to the Council and EU Parliament COM (2003) 771 final Development of the SIS II and possible synergies with a future Visa Information System (VIS), p 15

[31] Saas, Claire "Refus de deliverance de visa fondé sur une inscription au SIS", *Cultures et conflits* www.conflits.org/document.php?id= 917

[32] Note from Presidency to Working Party on SIS Requirements on SIS, Council Doc. 5968/02, 5.2.2002, p2

norms. In its less widely published texts the JSA, has noted this change, not without concern : "the JSA has warned that, as they stand, these proposals would result in a fundamental change to the nature of the system ... the SIS II looks set to become a multi-purpose investigation tool"[33]. This transformation is problematic "it is difficult to see how there can be a proper assessment of the potential implications of the SIS II when its development is to be so flexible that it is unclear what form the system will ultimately take ... [and] must also make it more difficult for those developing the system to take account of the principle of proportionality"[34]. No impact assessment of the SIS II was ever published by the Commission or Council, suggesting that no detailed consideration was given to the implications of the SIS II in terms of data protection or proportionality.

Specified, explicit and legitimate

Under the current provisions of Article 102 the executive action that will be taken pursuant to an alert is to an extent foreseeable to the data subject, but are the ever expanding functionalities lawful? The EDPS has acknowledged that "only a clear definition of purposes will allow a correct assessment of the proportionality and adequacy of the processing of personal data"[35]. Under the SIS II proposals, the interlinking of alerts and the merging purposes of informational assistance, executive action and investigative support jeopardise the data subject's ability to foresee the consequences of his or her actions, for either free movement or the protection of the right to a private or family life.

Relevant litigation is winding its way through national courts. The European Court of Justice case of Spain v Commission[36] concerns an action brought against Spain with regards to its administrative practice of refusing visas to all persons registered on the SIS without examining their circumstances on a case-by-case basis. It exposes a widely applied process whereby the SIS' function as informational support is overtaken by its automatic translation into executive action. The Court's decision in this case is awaited, as it represents the first such case before the ECJ. Until then, the administrative practices currently operating in certain member states will continue.

The French Conseil d'Etat case of Cucicea-Lamblot[37] examined whether the application of the Schengen Convention was compatible with the ECHR. The court held that a violation of Article 8 of the ECHR could be invoked against a decision to refuse entry under the Article 5(1) of the Schengen Convention. In order to review the refusal of the visa, the grounds on which the individual had been listed by the Greek authorities in the SIS had to be considered. These grounds had not been communicated to the applicant and the court ordered the Minister of Foreign Affairs to communicate, within two months, all relevant information. It held that domestic courts must know the grounds of a decision and the identity of its author to understand its consequences. If the decision of the authorities is unlawful according to the ECHR, the visa refusal will be quashed.

The collection and content of the data must be lawful to comply with the case law of the ECHR: "a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen (...) to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail"[38] Even assuming the collection, storage and transmission of data on the SIS is both necessary and proportionate to the objective of maintaining the free movement of persons in an area of freedom, security and justice, the national courts are obliged to consider whether there is sufficient foreseeability for the data subject.

The flexibility of the SIS II means data collection is used to deal with the latest policy bête noire. The unlimited functionality so desired by the Council and member states would seem unlawful, unless this breach of a person's right to privacy is within the exception provided by Article 8 ECHR: "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". Decisions in this field must, in so far as they may interfere with a right

[33] JSA Report Jan 2002 – Dec 2003 p 17

[34] Joint Supervisory Opinion on the development of the SIS II, 19.5.2004, p 3

[35] Opinion of the EDPS on the Proposal for a Regulation of the European Parliament and Council concerning the VIS and the exchange of data between Member States on short stay visas, COM(2004)835 final OJ C181/06, 23.3.2005 p17

[36] Case C-503/03 Commission of the European Union v Kingdom of Spain, Judgment 31 January 2006

[37] (Unreported, October 25, 2000) (CE (F)), case comment by Errera, Roger, *Public Law* 2001, SUM, 425-426

[38] Rekvényi v Hungary (Application no. 25390/94) ECHR, Judgment 20 May 1999

protected under Article 8 (1), be justified and proportionate to the legitimate aim pursued[39].

The ECHR case of Amann v Switzerland[40] provides guidance in the context of a card index database used to process surveillance information. In this decision the court held that both the creation of the card and its storage in the Confederation's card index amounted to interference with the applicant's private life. There had been a violation of Article 8 because national law did not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in gathering and storing surveillance and personal data.

The SIS II's compatibility with Article 8 and data protection standards is contentious, not least because of the interlinking of alerts and the effects of merging investigative, informational and executive purposes. This function creep has been gradual, with reasons for exclusion a political moving feast : the spectres of narcotics, crime, political dissent, criminalised migration and terrorism[41] have been used in turn for pushing back the boundaries of interference deemed necessary in the interests of security.

Structure and content

System architecture

At present, Article 94 of the Schengen Convention states that personal information held on the SIS is "no more than" [42] the surname, forenames and any aliases; any objective physical characteristics not subject to change; date and place of birth; sex; nationality; whether the persons concerned are armed, violent or have escaped; the reason for the alert; the action to be taken; and in cases of alerts under article 95, the type of offence. The SIS II proposals enable the data subject to be identified with more accuracy by also including on the name at birth, previously used names, fingerprints and photographs. The proposals provide more detail on the circumstances leading to the alert, including the authority that issued it and a reference to the judicial or administrative decision that gave rise to it.

The restriction imposed by Article 94 is undermined by the architecture of the system. The SIS is made up of the N-SIS, the national SIS databases in each country which are linked to the C-SIS, the central system based in Strasbourg. Member states supply information to the system from the N-SIS to the C-SIS which, through the SIRENE national bureaux, transmits identical information to the different N-SIS. When the SIRENE system is consulted for supplementary information pursuant to a positive hit, it must respond within 12 hours[43].

The Proposed Decision replaces the current C-SIS/N-SIS and provides that the national systems, NS, of member states will now connect to the SIS II via the NI-SIS which itself will provide one or two access points to the new central database, the CS-SIS[44]. The Commission appears to have decided on a "hybrid architecture with no data in the national interface"[45] : all data would be held on the CS-SIS with no information held on the NI-SIS. Member states could store data on their NS or access the SIS II directly.

Chinese walls and data laundering

One of the architecture's problems is that some of the most sensitive personal information is contained not on the C-SIS but on SIRENE. The SIRENE Manual[46] governs the organisation of the SIRENE bureaux and the process governing the exchange of information before during and after alerts and "hits". The information exchanged includes the type, date and authority of the decision, and may include supplementary information if requested. The SIRENE Manual was published in 2003, eight years after the SIS came into operation. The Annexes to the Manual, which set out the criteria for transmitting messages, such as when telephone conversations need to be confirmed in writing and the kind of supplementary information required, have not been published to date. There is an ensuing lack of foreseeability for the data subject.

The proposals state SIS II will be comprised of the CS-SIS, the NI-SIS and "the communication infrastructure" between them. Herein lies further scope for as yet undefined potential functionalities to creep through the system. The communication infrastructure, like the current SIRENE network, would consist of the contact between police,

[39] Beldjoudi v France 55/1990/246/317

[40] (Application no. 27798/95), 16 February 2000

[41] Council Communications SCH/Com-ex (93)9 and SCH/Com-ex (94)28 rev., and Note from EU Presidency to Council/Mixed Committee Council Doc 14790/01

[42] Article 94 Schengen Convention

[43] Sirene Manual OJ 2003/C38/09 12.2.2003

[44] Article 4(1) and (2) Proposed Decision

[45] Communication from the Commission to the Council and The European Parliament Development of the SIS II and possible synergies with a future VIS, COM(2003) 771 final, 11.12.2003, p13

[46] Sirene Manual OJ 2003/C38/01 12.2.2003

judicial, customs, vehicle registration authorities[47] and border agencies in different member states. It would include media both written and oral, and both recorded and unrecorded. It will be used for the exchange of supplementary information[48].

"Supplementary information" is defined as information not stored on the SIS II but connected to SIS II alerts which is *necessary in relation to the action to be taken*[49]. A (presumably new) SIRENE Manual will provide procedural guidance but its precise content will be decided at a later date by the Regulatory Committee on the basis of qualified majority[50]. Unfortunately, its publication is not expected to be imminent either. The content of supplementary information and the way it links to alerts has been omitted from Proposed Regulation, again because it would require details too technical and exhaustive to be included[51].

"Additional data" is defined as data stored in the SIS II and connected to SIS II alerts which is *necessary for allowing the competent authorities to take the appropriate action*[52]. This raises the question of whether additional data is data in addition to the exhaustive provisions of Article 16 of the same Proposed Regulation. The drafting's ambiguity is compounded by the definitions proposed in Article 4 : the difference between information *necessary in relation to the action to be taken*, and information *necessary for allowing the appropriate action to be taken* is moot. Europol, which has access to SIS information under the SIS + 1 proposals, has fallen foul of this nuance: in a 2002 note[53] to the Council it expresses that it could seek additional information from the SIS once a hit had been made. The Council is similarly confused in describing the information to be exchanged after a positive hit : "additional information may be the European Arrest Warrant or the additional information from the SIRENE bureau"[54] In confounding the two terms the Council and Europol point to the problem that the SIS is a poorly defined and very permeable structure, which authorities in different member states can in any event by-pass by contacting each other directly.

The other pillars of the SIS, the Consular Common Instructions ("CCI") and the Common Manual ("CM"), govern the conditions for issuance of a visa. They too were not published in the Official Journal for a number of years[55], and then were done so selectively, with gradual declassification beginning in 2000[56], five years after the system came into operation. As with the exchange of supplementary information under the SIRENE Manual, the conditions under which consular agents are required to contact other central or consular authorities and exchange information remain confidential[57] and unpublished, including the list of nationalities for which this procedure is carried out.

The CCIs provide for "additional documents" to be submitted in support of a visa application. These vary from country to country depending on local migratory risks[58]. They include information exchanged with a view to establishing that the applicant is a bona fide person, and thus subject to fewer checks[59]. There is also a certain amount of informal contact which includes the exchange of information both verbal (likely unrecorded) and written. The existence and exchange of such information is assured by the structure of the SIS, in this case without any corresponding data protection measures.

Guild refers to this volume of information as a "third system of information"[60] where the CCIs provide for no independent control of information circulating between different diplomatic or visa issuing posts and data protection authorities have no explicit powers to intervene.

Under the SIS II proposals this would represent a fourth system of information, the first three being the NI-SIS, the CS-SIS and the "communication infrastructure" provided by the SIRENE bureaux

[47] Proposed Regulation regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates COM(2005)237 final, 31.05.2005

[48] Article 4(4) Proposed Decision

[49] Articles 3(1) Proposed Regulation and Decision

[50] Article 61

[51] Recital 19, Proposed Regulation

[52] Articles 3(1) Proposed Regulation and Decision

[53] Note from Europol Council Doc 9323/02, 28.5.2002

[54] Note from Presidency on SIS II functions/Open Issues, Council Doc 12573/3/04, 30.11.2004 p7

[55] Decision of the Executive Committee of 28 April 1999 (SCH/Com-ex (99) 13) OJ L 239 22.9.2000 P. 0317 - 0404

[56] Council Decision 2000/751/EC

[57] Common Consular Instruction Annex 5b OJ C 313/1 and Common Manual Annex OJ C 313/97 16.12.2002.

[58] CCI Part V, #1.4

[59] CCI Part V, #1.4

[60] Guild, Elspeth, Le Visa : instrument de la mise à distance des "indésirables" , *Cultures et conflits* www.conflits.org/document.php?id=933

and SIRENE Manual (and subsequent incarnations). This fourth information system is not defined, not named, not verifiable, in some cases unrecorded. It is "a database that does not speak its name so as not to permit access to this database"[61]. The disparity in consular practice and the existence of hidden data beyond the overtly confidential data of respective Annexes 5b and 14b of the CCI and CM embed this fourth information system in the SIS and SIS II's architecture.

Both hard data, such as that referring to convictions, judgments and administrative decisions, and soft data relating to unconfirmed information, investigations and suspicions, are important in national authorities with the information required to perform their duties. Bearing in mind the wealth of supplementary information available on the SIRENE system as well as on local databases more loosely connected with the SIS, significant amounts of soft data will be available to end users. The Council's own example of spouses suspected of terrorism being included on the SIS with Article 96 alerts is an example of soft data and hard data being mixed.

This presents two major difficulties: the first is that soft data is more difficult to verify and update than hard data, posing significant doubts as to its accuracy in many cases. In the Netherlands, a 1999 report by its Court of Auditors revealed that much of the information contained on the Dutch N-SIS was contaminated, in part because the public prosecutor did not notify the police when charges against a suspect were dropped[62] and more generally because the system does not provide for registration of the results of investigations[63]. The practice of "data laundering"[64] also undermines the reliability of soft data, even that seeming to originate from a reliable source. If data is initially circulated through, for example, a law enforcement body, and that information is subsequently provided to another agency and then retained on that second database, the originator of the information can be obscured, resulting in an apparent confirmation of the information by two different sources. This creates a mirage where the data appears more reliable than it actually is, and can be given undue importance by the end user who has no way of checking either its real source or its accuracy.

The securitisation of migration

A deficiency inherent cross-border data processing initiatives is the heterogeneous nature of the procedures used in each member state for the inclusion, amendment and accessing of information. The latest country-by-country breakdown of SIS hits recorded by SIRENE bureaux[65] shows that Austria recorded 12,078 internal hits (hits recorded internally in response to an alert entered abroad) and 414 external ones (hits recorded abroad in response to a national alert). Germany recorded 2224 internal and 3718 external. One can draw limited conclusions from such comparisons. The number of internal hits recorded by Austria is the highest in the Schengen zone, but this may reflect higher incidences of SIS consultation or identity controls within the country or at its borders. It does not translate into an assumption that more SIS subjects are seeking to enter or remain in Austria.

In addition, some but not all member states include on the SIS under Article 96 the details of all failed asylum applicants, whether or not they left the country voluntarily once a final decision on their claim had been made. Whilst Italy and Germany practise this process, France does not. As a result Italy and Germany are responsible for more than three quarters of all Article 96 records. In a report by the JSA on Article 96 alerts entered by different national authorities, national data protection authorities revealed that on the German N-SIS in as many as 20% of cases "persons had been entered into the SIS only for the purpose of determining their current whereabouts, which does not justify an alert."[66] An individual whose asylum claim has been rejected by Germany may find themselves unable to enter the entire Schengen area even if the

[61] Guild, Elspeth, Le Visa: instrument de la mise à distance des "indésirables"

[62] Jelle Van Buuren (2003) "Les tentacules du système Schengen" *Le Monde Diplomatique*, March 2003 http://monde-diplomatique.fr/2003/03/VAN_BURREN/9970

[63] Report of the Netherlands Court of Auditors (Algemene Rekenkamer) on the National Schengen Information System 1997 http://www.rekenkamer.nl/cgi-bin/as.cgi/0282000/c/start/file=/9282400/modulesf/gxem5irq

[64] Submission by Justice to the House of Lords European Communities Committee (Sub-Committee F) on European Databases, April 1999, #6.16

[65] Note from General Secretariat on Table of hits recorded by the SIRENE bureaux for period 1 January 2002 to 31 December 2003, Council Doc 7915/04, 2.4.2004

[66] German Federal Data Protection Commissioner, Annual Report 2003/2004 of the Federal Commissioner for Data Protection, p22

reasons for their inclusion on the SIS would not be valid in most of the Schengen states.

The Proposed Decision also provides for the inclusion of European Arrest Warrants ("EWA") on the SIS II[67] and data on criminal prosecutions, both intended and actual, subject to the relevant limitation periods. The plans alarmed the EDPS: "the proposal does not contain all the necessary guarantees for an adequate data protection"[68] in conformity with European norms. The EDPS drew attention to the disparities in national legislation as regards the rights of data subjects in the exchange of information from criminal records[69], indeed common standards in this area have yet to be agreed. The Commission proposed legislation to create a benchmark for the exchange of criminal records in the form of a decision[70] but failed to yield a consensus amongst member states.

Den Boer explains that the complexity of management and decision making in the context of Europe's internal security has required many frameworks situated at numerous levels of governance and administration meaning that "enhanced cooperation in the criminal justice arena may already be a fact" [71]. In spite of divergence in practice and absence of common procedures, the process of exchanging information concerning police, border and criminal activities has already begun, both under the SIS as well as on an ad-hoc basis. The SIS and its successors are being pushed to reach beyond migration control and into day-to-day police and criminal justice activities. This link between migration, crime and national security is being forged without due regard to transnational data protection safeguards.

Biometric data

The biometric registration of all persons in the EU is an important objective of the EU policy[72]. The registration of migrants has been at the forefront of this process, with the creation of the Eurodac fingerprinting system for asylum applicants. SIS II proposals include the capability to store and exchange both fingerprint and photographic information, and a degree of access to the Eurodac database itself. An "Input Mask" has been developed[73] with reference to an existing Interpol input mask to capture information such as personal data, the Schengen ID number and that familiar creature, additional information.

Iris recognition technology is already in use in certain member states[74], but has not yet been deemed a practicable reality on an EU wide level. The schemes currently operate on a voluntary basis for highly skilled third country nationals, long term residents EEA and Swiss nationals. The technology is being piloted with low-risk, financially secure migrants. Once the systems are shown to be working effectively, iris recognition technology is likely to become more widely used, and used in cases involving forced migrants, or those assessed to be high-risk or undesireable.

The inclusion of biometric information in the SIS makes it an attractive source of information for a large number of both private and government institutions : the appeal of biometric data and the flexibility of the purposes to which it could be used "makes the prospect of function creep more likely"[75]. The pressure on the SIS is substantial, yet no data protection impact assessment of the system was ever made. The EDPS found that "the inclusion of biometric data involves a variety of practical problems that have yet to be resolved (the way in which biometric identifiers will be collected, for example) and until detailed plans have been proposed it is difficult to know what additional safeguards might be needed."[76] Data

[67] Article 15 Proposed Decision

[68] Opinion of the European Data Protection Supervisor,13.1.2005 #11

[69] Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the exchange of information from criminal records, COM (2004) 664 final of 13 October 2004,13.1.2005 #10

[70] Proposal for a Council Decision on the exchange of information from criminal records, COM (2004) 664 final of 13 October 2004,13.1.2005

[71] Den Boer, Monica (2004) Paper on Plural Governance and EU Internal Security: Chances and Limitations of Enhanced Cooperation in the Area of Freedom, Security and Justice,Oslo, 25.5.2004, p 11

[72] Draft Council Regulation on standards for security features and biometrics on passports and travel documents, Council Doc 15139/04, 23.11.2004

[73] Note from Netherlands, German, Austrian and Belgian delegations on SIRPIT (Sirene Picture Transfer) – SIRENE Procedure, Council Doc 9450/02, 30.5.2002, p5

[74] IRIS recognition programmes in operation include the frequent traveller processes at Heathrow in the UK, Schipol in the Netherlands and at Frankfurt Airport in Germany

[75] JSA Report on the development of SIS II, SCHAC 2504/04, p6

[76] JSA Report on the development of SIS II, SCHAC 2504/04, p6

protection appears to be an afterthought in EU policy to expand the SIS, a strategy that carries significant risk.

An important limitation on the effectiveness and fairness of including biometric data in the SIS is technological. At border control and in many police activities, searching for information held on the SIS needs to be an instant process. Including biometric information as an identification system (a one-to-many comparison or "fishing expedition") rather than a verification system (a one-to-one comparison) will slow down the system. The SIS + 1 is as yet incapable of supporting the exchange of fingerprint information, and it is uncertain whether the capacity for an instant response system will exist by the time SIS II is due to be activated. System delay must not result in agencies merely checking the data contained on the NS (which may be out of date) rather than awaiting the results of a search through the NI-SIS and CS-SIS.

Fingerprint data carries with it statistically important limitations. Up to 5% of persons are estimated to have no readable fingerprints or no fingerprints at all. Furthermore, an error rate of 0.5 to 1% for biometric identification systems is normal[77]. In terms of numbers of persons this could affect in any year, up to 1 million may not be able to follow the normal, biometric identifier-led application system, and between 100,000 and 200,000 people a year may be rejected on the basis of an inaccurate identification. The stigmatisation by judicial, police or immigration authorities and nefarious impact on freedom of movement remain possible consequences of undue reliance on fingerprint data.

The Prüm Convention[78] , also known as Schengen III, was signed in Germany on 27 May 2005 by certain member states and is worthy of a mention at this stage. It mirrors the SIS in its design and functions but is directed at Community citizens and EU nationals alike.

It includes provisions for the obligatory processing of the DNA data of its subjects where "circumstances give reason to believe that the data subjects will commit criminal offences at a political or sporting gatherings or pose a threat to public order and security".[79] Like the Schengen Convention, this agreement's intergovernmental roots will avoid parliamentary resistance and may yet cause problems for data access even after it is incorporated into EU law. Strong lateral cooperation between dominant EU member states has again forestalled EU democratic processes.

Troublemakers and Aliens

The prohibition on including information relating to religious belief, sexuality or political persuasion, except in the most limited of circumstances, is provided by all relevant data protection legislation[80]. The use of the SIS to restrict access to those attempting to demonstrate at G8 gatherings or international summits is at odds with this prohibition. The decision by a member state to curtail free movement rights under Article 2(2) [81] of the Schengen Convention is a matter of national sovereignty not requiring Community agreement, and thus unlikely to be challenged. France has invoked these measures more than any other EU country, in reflection of its general reluctance to lift controls on internal borders evident from 1995 onwards. In practice these measures have mainly applied to EU citizens and long terms residents seeking to participate in demonstrations or other legal activities[82]. The re-institution of internal controls for political gatherings motivated 16 out of 26 incidences where border checks were temporarily reintroduced in the Schengen area between 2001 and 2003[83].

Public protests expressing political dissent are merged with a new category of undersireable : "violent troublemakers". A draft Resolution put forward by the Italian EU Council Presidency in 2003 to deal with inhibiting the free movement of demonstrators[84]. Whilst these include "hooligans" with criminal records, they also include the politically suspect, for example those seeking to

[77] EDPS Opinion on the Proposal for a Regulation of the European Parliament and Council concerning the VIS , COM(2004) 835 final OJ 23.7.2005 C181/12, p 20

[78] Signed by Belgium Germany, Spain, France, Luxembourg, the Netherlands and Austria 10900/05, 7.7.2005

[79] Article 14

[80] Article 6 Convention 108, article 8 Directive 95/46/EC and Article 10 Regulation (EC) 45/2001

[81] Article 2(2) Schengen

[82] Groenendijk, Kees "Reinstatement of controls at the internal borders of Europe : Why and against whom?" in *European Law Journal*, Vol.10 No. 2, March 2004, pp150 - 170, p168

[83] Bunyan, Tony , Plan to put protestors under surveillance and deny entry to suspected troublemakers, Statewatch article: RefNo# 6952, August 2003 http://database.statewatch.org/protected/article.asp?aid=6952

[84] Draft Council Resolution on security at European Council meetings and other comparable events, Council Doc. 10965/03, 30.06.2003

protest at international political gatherings. It proposed to enable border checks to be instituted to identify those who are "believed to be intending to enter the country with the aim of disrupting public order and security at the event"[85]. There is a striking absence of any requirement for *serious*, or even *reasonable* grounds for believing that an individual intends to be a violent troublemaker. Grounds for exclusion are therefore subjective, and could include unreasonable or unfounded beliefs. It could suffice for an individual to be suspected of being a member of a political organisation that espouses direct action or protest, or be associated with an individual who is a member. With the purposes of the SIS II and this draft resolution so closely aligned, the Italian proposal bears resemblance to what the Commission might call a proposed SIS II functionality in the making.

Despite the invocation of serious crime and violence to warrant the biometrification and control of data on individuals, impeding free movement on a large scale has mostly been a tool of political control : "the authorities evidently deem controls at internal borders not be an efficient instrument in the fight against serious criminal activities unrelated to political events"[86].

The public policy justification for SIS II exclusions is a case in point. The infrequent use of Article 2 (2) overall reflects that reintroduction of border controls is mainly a symbolic enactment of national sovereignty, subject, in the case of EU citizens and third country nationals with free movement rights, to control by the ECJ. The SIS II is a site of great potency in controlling those within, as well as those seeking to cross the EU's borders.

The provisions for excluding or limiting the movement of persons are not just applicable to third country nationals. Although these cases have not been publicly acknowledged or pursued by the JSA, there are NGOs and lawyers who report that some of their clients, French nationals, "have been registered on the SIS even though this is formally prohibited on the basis of Article 96 which concerns undesireable aliens"[87]. The Proposed Regulation also purports to apply only to third country nationals[88] but it is difficult to ascertain how the new system will be able to exclude its application from EU nationals. This is particularly so in the context of the Spanish proposal that the SIS should have anti terror functions : the London bombings and the Stockwell shooting brought doubt to facile assumptions about nationality and threats to public safety.

The nebulous character of supplementary information disguises the inclusion of personal information regarding EU nationals. Personal information on EU nationals will be held on the SIS and its successors where that individual has sponsored a third country national's visa or residence permit application, is the spouse, child or parent of the third country national, or is travelling in the same group as the applicant. The inclusion of soft data and the linking of alerts will also enable information to be captured very widely. At the time the entry is made on SIS there is no way of knowing that at the time the individual seeks to enter the Schengen area, they have not come to benefit from Community rights. With EU nationals already included in the data to be migrated from the SIS and SIS + 1, and the increased interlinking of alerts, those benefiting from Community rights are likely to continue to have their data protection rights, if not their right of free movement, affected by the SIS.

In the Commission v Spain case referred to above the Court differentiates between the enhanced rights of those with EC free movement rights, and those without. In this case, at the time the applicants' details were entered on the system they had not come to benefit from EC free movement rights. The Court found that under Directive 64/221[89] a refusal must be based not on the mere existence of an entry on the SIS or a previous conviction, but on the personal behaviour of the individual. Derogation from the principle of free movement and right to family life is only possible if the presence of the individual in that area constitutes a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society[90]. Spain had therefore failed to fullfill its obligations under Directive 64/221.

This two tiered system of rights has been adopted by the Commission in the Draft Regulation. The

[85] Article 2

[86] Groenendijk, Kees (2004), pp150 - 170, p159

[87] Guild, Elspeth "Désaccord aux frontières et politique des visas : les relations entre Schengen et l'Union" *Cultures et conflits* www.conflits.org/document.php?id=927

[88] Article 15 Proposed Regulation

[89] Directive 64/221/EC OJ L 56, 04.04.1964 and other related free movement provisions such as Directive 68/360/EC are to be replaced by Directive 2004/38/EC OJ L 257 , 19/10/1968 P. 0013 - 0016 on 29.4.2006, but this change should not impact on free movement rights as applied in the context of Article 96 alerts.

[90] #53

ECJ's decision on the process for finding an infringement of Directive 95/46/EC and the way it relates to a breach of Article 8 ECHR[91] show that an approach should begin with an examination of national law and its compliance with European provisions. If European data protection standards are not met the measures' compliance with the requirements of Article 8 are also called into question.

Adequate, relevant and not excessive

Convention 108, Directive 95/46/EC and Regulation (EC) 45/2001 provide that the information held and exchanged through the SIS must be adequate, relevant and not excessive for the purpose of ensuring public and state security. The leaking of soft data into the SIS has already begun, and is likely to increase with the SIS II. The permeability of additional data, supplementary information and the "fourth information system" suggest that after a hit, authorities would have access to significant amounts of superfluous and unverifiable data. In addition, variations in national practices as regards the reasons for registering an alert suggest that some countries are including information deemed irrelevant by other member states. It is difficult to argue that such information is not excessive, when no EU consensus exists to support its inclusion.

Under the Schengen Convention, personal data should be kept only for the time required to achieve the purposes for which it was supplied, and its retention reviewed no later than three years after the information was included[92]. SIRENE data must also only be kept for such time as required to achieve the purposes for which it was supplied and must be deleted in any event no more than one year after the alert to which it relates has been deleted[93].

The Convention's provisions on the deletion of information have not succeeded in safeguarding the quality of the data held on the SIS. This is partly due to the provisions contained in the SIRENE Manual, which meekly suggest that "As far as is possible, these additional pieces of information should not be kept by the Sirene's once the corresponding alert has been erased"94. The JSA declared this provision in breach of the Schengen Convention95 : the use of data archived for monitoring or technical support purposes to prepare new documents relating to criminal or other matters is likely to constitute a departure from the principle of finality contained in Article 5(2) of Convention 108. In addition, "The existence of a monitoring system after deletion of an alert (...) does not justify archiving documents for an unlimited period of time"[96]. Unless the procedure in the SIRENE Manual or its successor can provide for such limits it will be in breach of this principle.

The German Federal Data Commissioner's Report of 2003/2004[97] on German N-SIS data reveals a number of shortcomings. In many cases, there was no record of a review as mandated by Article 112 to determine the need for continued storage of personal data. It was often impossible to determine how long an alert had been in effect due to a lack of documentation. In some cases, alerts had remained active for up to nine years. In nearly 50% of cases, the time limit for the alert in the SIS was linked to a permanent national ban on entry, and therefore not issued for a limited period of time. Lastly, deleting the alert in the SIS did not always entail deleting the records on which it was based.

Individuals currently have limited rights to access information held on them in the SIS[98]. They have a right to correct such information or to have it deleted if it is held unlawfully, or to seek compensation. They can also ask a national data protection authority to check the information held on them in the SIS[99]. These provisions are mirrored by the Proposed Regulation and Directive. Under the Proposed Regulation individuals would gain the right to review or appeal a decision to issue and alert[100] but the modalities of review or appeal are not expressed,

---

[91] Joined Cases C-465/00, C-138/01 and C-109/01, Rechnungshof, Osterreichischer Rundfunk and others, Judgment of the Court, 20.5.2003 (1)

[92] Article 112 Schengen Convention. Debate as to whether Article 113 applied instead (where the maximium period of retention was 10 years) was convincingly settled by the opinion of the JSA Opinion Concerning the relation between Articles 112 and 113 Schengen Convention SCHACH 2510/1/02 REV1, 7.10.2002

[93] Article 112A Schengen Convention

[94] SIRENE Manual # 2.1.3(b).

[95] Recommendation from the Schengen JSA SCHAC 2505/99 LIMITE, 11.10.1999

[96] Recommendation from the Schengen JSA SCHAC 2505/99 LIMITE, 11.10.1999 p3

[97] German Federal Data Commissioner Report 2003 2004, www.bfd.bund.de/information/tb04_engl.pdf, pp22-23

[98] Article 109 Schengen Convention

[99] Articles 110 and 111 Schengen Convention

[100] Article 15(3) Proposed Regulation

nor is any remedy, penalty or requirement as to suspensive effects over removal measures.

Data subjects are currently prevented from accessing information held on them in the SIS if it is indispensable for the performance of an action connected to the alert or to protect the rights and freedoms of others. This restriction is lifted in the Proposed Regulation. Regulation 46/95/EC[101] does contain loose grounds for restricting access (in the case of public security or the protection of rights and freedoms of others) which should nonetheless apply. The current right to ask a supervisory authority to verify data in cases where individuals have been refused access is absent in the Proposed Regulation. This blunts the teeth of the EDPS. The interlinking of alerts is also pertinent to data subject access, as it renders the application of a 'blue pencil' test, whereby restricted and available data are severed, problematic.

The right to be informed when an alert is issued in a person's regard remains absent in the proposals. The right to compensation for illegal or incorrect entries is delegated to national law, where judicial systems may not be accessible to those denied entry to the EU. The applicant's need for territorial presence to access the courts is necessary for actions in respect of the SIS II's immigration provisions under the Proposed Regulation[102], but not for actions under the Proposed Decision. The discrepancy in territorial provisions may be resolved by the final drafts but unless they are settled in the applicant's favour, the data subject's access to justice will be inhibited.

A 2002 French case[103], unreported, concerns the exercise of national data supervisory authorities' powers to access and verify information on the SIS. In this case, Mr Moon and his wife were refused entry by France on the basis of an information input by another member state. Mr Moon, not permitted to verify the information himself, asked the Commission nationale de l'informatique et des libertés ("CNIL") to do so on his behalf. In its response the CNIL confined itself to confirming the information had been verified. The court held that the fundamental rights of access and rectification were deprived of practical value by the curtness of the CNIL's answer, and ordered the CNIL and the Minister of the Interior to communicate to it within two months all elements relating to the reporting of Mr Moon on the SIS, and justify any non disclosure. A second ruling[104] on the case confirmed that France did not have the power to amend another member state's entry, but could call the other member state to account for correctness of that entry. Errera highlights the influence of international instruments in this decision as another illustration of the internationalisation of the law relating to data protection. Nevertheless, with 5 years elapsing between the refusal of entry and the court's ruling in this matter, the pace of legal action, even in national courts, impedes the effectiveness of current remedies.

These are flaws with adverse effects quality. Garbage in - garbage out, the expression goes, and with over 125,000[105] SIS access terminals in existence there is strong potential for inaccurate information to be disseminated through a vast geographical, administrative and operational space. The accuracy of some of the information contained on the SIS is already in doubt. Delegating responsibility to national authorities has not resulted in a reliable mechanism for ensuring data quality. The sheer quantity of information contained may seem an advantage in immigration decisions and criminal prosecutions, but it undermines the very accuracy of that data.

Widening access

With the pressure on the SIS to yield up information to police and judicial authorities, one effect on the SIS has been the widening of those permitted to access and amend the information it contains. The SIS+1[106] expanded access to the SIS : where the right to search data directly was exclusively that of authorities responsible for border control and in-country police checks, it can now be accessed by national judicial authorities with a view to prosecuting, or making enquiries prior to indictment. At present, only those authorities notified pursuant to Article 101(4) of the Schengen Convention are allowed to search the SIS directly. The list of these authorities was most recently published on 10 December 2004[107]

[101] Article 13

[102] Article 31(1)

[103] Moon, Re (Unreported, November 6, 2002) (CE (F)) Conseil D'Etat (Assemblée), case comment by Roger Errera, *Public Law* 2003, SPR, 187-190

[104] Moon (2 June 2003) CE Decision n° 194295

[105] Statewatch Analysis, SIS II: fait accompli? http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf

[106] Article 101, as amended

[107] 16023/04 SIRIS 144 COMIX 768 List of competent authorities authorised to search directly the data contained in the Schengen Information System pursuant to Article 101(4) of the Schengen Convention

and overall, police, border guards and judicial bodies are already authorised to access and amend all data processed under articles 95 - 100. For the most part, immigration authorities within the country plan to gain access to Article 96 alerts only.

In reality, the existence of these 125,000 access terminals and the increasing number of bodies and member states permitted to access them makes compliance with the Schengen Convention's confidentiality requirements difficult. In 1998 a written question by a Greek MEP revealed that SIS information had been leaked by Belgian police to local gangs.[108] A 1999 report by Justice on European Databases described procedures in the Netherlands, where the rooms housing the Interpol computer terminals and the SIRENE terminals are "adjacent, separated only by a smoked glass partition and open door. SIS operators work a 24 hour shift system, whereas those on Interpol terminals work regular office hours; SIS personnel handle any important Interpol business during off-hours"[109]. A comprehensive account of practices in different members states would provide much needed information for an EU wide assessment of the operational risks and processes..

UK and Ireland's access to Article 96 alerts

UK and Ireland participate selectively in the Schengen acquis[110] including SIS provisions, save those concerning Article 96 alerts. Cross border police activities, however, are within UK participation.[111] It has not been conclusively decided which UK agencies will access the information and to what extent the UK will effectively continue to exclude application of Article 96 of the Schengen Convention. This ring-fencing of Article 96 alerts from access by the UK and Ireland goes against the obligation under Article 92(2) of the Schengen Convention for the different N-SIS to be identical in content. Article 94 limitations on the use of data are removed in the SIS proposal and indications on how the interlinking of alerts will comply with limitations on access have not yet surfaced in the morass of documents currently listed on EU registers.

The JSA rejected the UK solution of allowing all information to be accessed by a few select individuals in the UK N-SIS, being in breach of the Schengen Convention. The Dutch solution to place a filter at the C-SIS level to prevent the transmission of Article 96 information to the UK and Ireland whilst providing a facility to check for double alerts was accepted[112]. The JSA expressed that any option must also comply with the data protection principle enshrined in Article 94, but the proposals mean the UK and Ireland's future participation in the SIS risks contamination by Article 96 data and alerts.

Exchange of information with third parties

The Council introduced Decision 2004/496/EC[113] requiring air carriers flying to, from or over the United States to provide United States Department of Homeland Security, Bureau of Customs and Border Protection with electronic access to information held on passengers. This is a "pull" system, with US authorities entitled to request and receive information from carriers. To comply with Directive 95/46/EC the Commission adopted Decision 2004/535/EC in which it decided that US authorities provided adequate data protection measures. This cleared the way, or so it thought, for the wholesale transfer of passenger data contained on carriers' information systems to US customs and internal security agencies. These Decisions have been controversial. The European Parliament submitted conclusions to the ECJ[114] to annul the agreement and the Decisions and the EDPS has now been granted permission[115] to support the European Parliament in its action.

The Parliament argues that because the agreement entails the transfer of sensitive data in breach of Article 8 of Directive 95/46/EC, an amendment of that Directive is implied. The co-decision of the European Parliament should therefore have been obtained and the decisions were therefore ultra-vires. Furthermore, the agreement constitutes an unjustifiable

[108] Written question No. 19/98 by Nikitas KAKLAMANIS to the Commission. Official Journal C 196 , 22/06/1998 P. 0107

[109] Submission by Justice to the House of Lords European Communities Committee (Sub Committee F) on European Databases, April 1999, p11

[110] as referred to in Article 1(2) of Council Decision 1999/435/EC

[111] Council Decision 2000/365/EC

[112] Note from the Chairman of the JSA to the Chairman of the Article 36 Committee, SCHAC 2502/2/02 REV 2, 11.3.2002, p6

[113] Council Decision 2004/496/EC on the conclusion of an Agreement between the European Community and the USA on the processing and transfer of PNR data by Air Carriers to the US Department of Homeland Security Bureau of Customs and Border Protection

[114] Case C-317/04. European Parliament v Council of the European Union and Case C-318/04 European Parliament v Commission of the European Communities

[115] Case C-317/04 Order of the Court (Grand Chamber) (Intervention), 17.3.2005

interference with private life and is thus incompatible with Article 8 of the ECHR. The breach arises through the transfer of large volumes of information to a third party without the consent of the persons concerned, and without providing a way of controlling the consequences of the transfer[116]. On account of the excessive amounts of data processed, and because the US authorities hold the data for too long, the measures are not proportional. Lastly, the hurried implementation of the decisions, which failed to await an opinion by the ECJ requested by the Parliament, is in breach of the Community law principle of cooperation in good faith. This case will test the effectiveness of the EDPS and the European Parliament, and represents a real challenge to the political imbalance in community procedures..

The EU has now agreed similar measures with the Canadian authorities albeit under a "push" system. Here, the EDPS approved[117] the main elements of the agreement. In this case, the measures provide for more limited data to be transferred which does not include of open-ended categories of personal and potentially sensitive information. Despite its developed system of data protection, Canada cannot ensure compliance with Directive 95/46/EC in granting full protection to EU citizens, and the EDPS calls for amendment of the agreement in that respect.

As with the SIS, the list of national authorities with access to the SIS II must be notified under the Proposed Regulation. For Article 15 (1) refusal of entry alerts this would include authorities responsible for the implementation of an elusive Directive 2005/XX/EC "for the purpose of identifying a third country national staying illegally in the territory in order to enforce a return decision or removal order."[118]

Proposals for Directive 2005/XX/EC have yet to exist, making it impossible to evaluate the impact of this provision, although one suspects it aims to lower the benchmark for inclusion to encompass individuals subject to immigration refusals. Third parties could include private organisations because this option is not excluded by the Proposed Regulation and Decision[119].

Europol and Eurojust

Europol, the non-executive agency set up by the Europol Convention to facilitate the exchange and analysis of criminal intelligence between member states, third states and organisations. As part of the Spanish initiatives, in June 2005[120] Europol was granted access to Article 95, 97 and 99 data, and Eurojust to Article 95 and 98 data, a measure the Council had been considering since 2001[121]. These agencies have also been granted access to SIRENE supplementary information.[122] In line with its tendency to agree new functions before deciding the legal or technical limitations required, in May 2005[123] the Council was still undecided as to whether Europol would access the SIS through a Dutch IT provider, through re-using existing native N-SIS, through daily import of N-SIS content, or through a copy of the C-SIS database. Europol's access would be on a "hit / no hit" basis and with Europol able transfer the data from the Europol Information System into the SIS II. This process will bring the information systems into alignment, but it does also create a risk of data laundering.

The limitation imposed on the purposes for which these agencies can access information is removed through the linking of Article 96 alerts to those under other articles[124]. Furthermore, access is permitted so long as it is *necessary for the performance of Europol and Eurojust's tasks*. This is a wide definition that has come under criticism by the Schengen JSA: "there ought to be clarification of the specific tasks for which Europol, Eurojust (and any other organisations) require access to the SIS II"[125]. In the UK, the House of Lords Select Committee on European Union expressed concern that the provisions will lead to a significant change in the powers of Europol and Eurojust. They would be extended access to the SIS even though their respective instruments do not provide for such a possibility.

[116] Ordonnance du Président de la Cour, 21.9.2004, in case C-317/04, #5

[117] Opinion of the European Data Protection Supervisor on the Proposal for Council Decision (COM)(2005) 200 final, 1.5.2005

[118] Article 18 Proposed Regulation

[119] Explanatory Memorandum of Proposed Directive COM(2005) 230 final, p3

[120] Article 1(9) Council Decision 2005/211/JHA

[121] Communication from the Commission t the Council and the European Parliament, Development of the Schengen Information System II, COM(2001) 720 final, 18.12.2001, p7

[122] Articles 33(3) and 18 (2) Proposed Decision

[123] Note from Presidency on Mandate for a technical analysis concerning the implementation of Article 1(9) of Decision 2005/211/JHA - Access to the SIS for Europol, Council Doc 8874/05

[124] Note from Presidency on SIS II functions/open issues, Council Doc 12573/3/04, 30.11.2004, p3

[125] JSA opinion on the development of SIS II, SCHAC 2504/04 p4

"The absence of such a mandate is particularly striking (...) The only provision that enables Eurojust access to SIS data appears to be an unpublished non-legally binding declaration annexed to the Eurojust Decision (which we have asked to see but have never received)."[126] Furthermore, whilst Europol is permitted to request and receive information from third states and organisations, the Europol database cannot be connected to any other system directly. The Proposed Decision states that Europol may not connect to or download or otherwise copy any part of the SIS II[127]. These provisions are a fig-leaf if Europol can access NS information, which could include copies of SIS II information entered on the system by different member states, directly.

Can Europol's compliance with the measures set out in the Schengen Convention be assured when Europol is not itself bound by the Convention? Europol admits that accessing the database will breach these limitations: "Regarding the usage limitation set out in the Articles 95 - 100 for each of the categories of reports and data, it is clear that Europol cannot fulfil these requirements"[128]. This arises in part because Europol is a non executive agency and therefore unable to perform the task required once a positive hit is made. The Council seems unconcerned with such legal details. One solution proposed was for Europol to become a signatory of the Schengen Convention[129], but this has been discarded, and it was decided that Europol will be given the status of a special (limited) end-user. Europol suggested that : "The search by Europol officials in the SIS should be considered as an administrative check and a positive result should be considered a "discovery" rather than a hit"[130]. In opting for this uneasy solution, Europol may have given consideration to Article 102(4) of the Schengen Convention which states that data may not be used for administrative purposes. At present there are no effective means of ensuring Europol meets its obligation to adopt reciprocal security and confidentiality provisions in its communication of the information to third parties.

The data should only be transferred by Community bodies to recipients who can assure an adequate level of protection[131], but with the "adhocratic and contradictory character of lawmaking in this area" detailed by Guiraudon[132], there is scope for disjunction between discourses and legal processes in different EU organisations and member states. A normative application of data protection guarantees needs further specification, even if some case by case design is inevitable, due to the technical requirements and functionalities of data processing needed in different contexts.

Interoperability

The Council has developed a Visa Information System ("VIS") [133] to hold personal and biometric data for all persons who apply for visas to enter the Schengen area. The VIS links the applicant's record with that of group members travelling with the applicant and family members. It is proposed that the VIS and SIS II share a common platform, with data stored on the same system and accessed by the same end users. The VIS' structure is similar to that of the SIS, comprising of the central level CS-VIS which interfaces with the national level NI-VIS and local agencies, including diplomatic posts, borders, and immigration and police authorities. The European Parliament was consulted on this proposal and rejected it. The Council succeeded in by-passing the co-decision procedure which would have been required by a regulation.

The Meijers Standing Committee of experts in international immigration, refugee and criminal law has levelled criticisms at the VIS[134] which echo those of SIS II proposals. A fully informed assessment of the system was (once again)

[126] Letter from the Chairman to Bob Ainsworth MP, Under-Secretary of State, Home Office, Written Evidence of the House of Lords Select Committee on European Union, Schengen Information System : New Functions (Council Doc 9407/02 and 9408/02), 9.4.2003

[127] Article 57(7)

[128] Note from Europol (Legal) issues raised during the last session of the EU Working Party SIS in relation to access to the SIS for Europol, 9323/02, 28.5.2002, p6

[129] Communication from the Commission to the Council and The European Parliament Development of the SIS II and possible synergies with a future VIS, COM(2003) 771 final, 11.12.2003, p5

[130] Note from Europol (Legal) issues raised during the last session of the EU Working Party SIS in relation to access to the SIS for Europol, 9323/02, 28.5.2002, p6

[131] Article 9 Regulation (EC) 45/2001

[132] Guiraudon, Virginie, (2001) *The EU "garbage can": Accounting for policy developments in the immigration domain*, p38 http://www.eustudies.org/GuiraudonPaper.do

[133] Council Decision 2004/512/EC OJ L 213 of 15.6.2004, p. 5

[134] Comments Standing Committee on the draft proposal for a Regulation concerning the VIS, COM (2004) 835, April 2005, http://www/commissie-meijers.nl

impossible to make, but the Committee found that the EDPS lacked the facilities to properly monitor data protection, and was critical of Article 3 of the draft regulation, which provides for links to "other" (undefined) applications.

The SIS II will interconnect with the VIS, Europol Information System and Customs Information System. It will be accessed by vehicle registration authorities, as well as police, border and judicial bodies. It will be linked with third states and organisations. It will be linked to shared data platforms such as the Communication and Information Resource Centre Administrator (CIRCA). This integration of databases is leading to a widening of police powers[135] and points to a danger of interoperability - that it creates the possibility for an authority, denied access to certain data, to obtain access to it via a different information system. The Commission estimates that the VIS alone will handle approximately 20 million visa applications per year. Information relating to these applications can be stored for up to 5 years. This represents vast data, and data with a data protection regime which gives rise to serious concern. "To modernise immigration policy at the cost of dehumanising it"[136] is the effect of an asymmetry in policy development where control of migrants is extended without a corresponding development of their rights.

Conclusion

In 2004, the cost of creating and operating the C-SIS amounted to more than €23,500,000. The C-SIS operating costs for 2006 are estimated to be over €2,000,000 annually[137]. This is a significant investment even without including the costs born by member states in operating the N-SIS, the expanded functions and interoperability of the system, or the effects of nearly doubling the size of the SIS to integrate Europe's acceded states.

The cost for data protection in the EU is also heavy. The function creep brought about by linking alerts, and expanding the content, interoperability and access to the SIS is entrenched by proposals for the SIS II. The porous, ill-defined and expansive nature and purpose of the SIS II is a structural weakness. It fuses hard and soft data and necessarily undermines the system's ability to deal accurately and lawfully with the increase in information processed on the system. The SIS II project is, even the national technical delegates admit, in trouble[138]. The Commission itself stated that the technical proposal was "of such bad quality that the Commission did not want to discuss it"[139]. The data quality of the SIS is certainly flawed and the data subject has scant hope of accessing or even amending the information contained. "Hard law" proposals such as the Proposed Regulation and Decision provide a pressing opportunity to develop better norms and procedures. The decisions of national courts, the European Court of Justice and the European Court of Human Rights have also helped the emergence, albeit at a very slow pace, of a jurisprudence on the SIS that provides grounds for challenging its compliance with data protection and human rights norms. In developing the principles of proportionality and foreseeability, the courts have shown the beginnings of a procedure for enforcing international data protection norms at a local level. The EDPS has also been ready to use its judicial and reporting roles to improve compliance of the SIS with data protection standards at an EU level.

A degree of defeatism is inevitable if the SIS II's proposals are taken in their entirety and one looks into the depths of EU document registers to discover that, in so many ways, it already exists. The intergovernmental origin of the Schengen Convention and the uncertainty surrounding the legal basis of SIS have enabled the development of the SIS and SIS II to be lost in large numbers of disparate non-binding documents produced by the Council, Commission and Presidency. The SIS II and now the Prüm Convention are vivid examples of how the Schengen Convention has already returned to haunt the citizens of the EU. Data protection is secondary to data surveillance in this regime.

The SIS II proposals raise several issues, but debate and attention could be focused on amending the Proposed Regulation and Decision in three principal ways. for excluding or expelling individuals from the EU should be removed. Soft data should be qualified as such and its use and

[135] Salter, Mark (2004) "Passports, Mobility, and Security: How smart can the border be?" *International Studies Perspectives* (2004) 5, 71–91, p87

[136] Baldwin-Edwards, Martin (1997) Thee emerging European immigration regime: some reflections on implications for Southern Europe, *Journal of Common Market Studies*, Vol. 35 No. 4, December 1997, p 513.

[137] "I/A" Item note from General Secretariat on C.SIS installation and exploitation budged for 2006 Council Doc 8997/05, 27.05.2005

[138] Note from Presidency on Assessment of the state of the SIS II project Council Doc 9672/05, p 1

[139] Note from Presidency on Comments on the Commission's progress report for SIS, Council Doc 8506/0, 27.4.2005, p2

exchange regulated through measures to amend the SIRENE Manual, CCIs and CM approved by the European Parliament. There should be acknowledgement of the effects of the measures on both EU nationals and persons with Community rights. The EDPS should be granted powers to access, verify, amend and report on SIS II data in a manner that is transparent and available to persons in the EU or excluded from its territory.

With the use and transfer of supplementary information and that contained on the fourth information system, the SIS reaches into the borders of Europe to be used against EU and third country nationals alike, in investigations at local level by national agencies in the course of their normal police and judicial responsibilities.

The expansive application of the public policy basis for refusing entry to the EU represents a dangerous mutation in the subjective notion of a threat to security.

Bibliography

Amann V Switzerland (Application no. 27798/95), 16.2.2000

"I/A" Item note from General Secretariat on C.SIS installation and exploitation budged for 2006 Council Doc 8997/05 SIRIS 44 COMIX 326 OC 287, 27.05.2005

Baldwin-Edwards, Martin (1997) The emerging European immigration regime: some reflections on implications for Southern Europe, *Journal of Common Market Studies*, Vol. 35 No. 4, December 1997, p 513.

Beldjoudi v France 55/1990/246/317, 26.2.1992

Bunyan, Tony (2003) Plan to put protestors under surveillance and deny entry to suspected troublemakers, Statewatch article: RefNo# 6952, Statewatch News Online, August 2003 http://database.statewatch.org/protected/article.asp?aid=6952

Case C-317/04 Order of the Court (Grand Chamber) (Intervention) European Parliament v Council, 17.3.2005

Case C-317/04. European Parliament v Council OJ 11.9.2004 C 228, (2004/228/66) 27.9.2004

Case C-318/04 European Parliament v Commission Action OJ C228 (2004/228/67) , 11.9.2004

Case C-503/03 Commission v Kingdom of Spain, Judgment 31 January 2006

Comments Standing Committee of experts in international immigration, refugee and criminal law on the draft proposal for a Regulation concerning the VIS, COM (2004) 835, April 2005, http://www/commissie-meijers.nl

Commission Communication to the Council and EU Parliament Development of the SIS II and possible synergies with a future Visa Information System (VIS), COM (2003) 771 final 11.12.2003

Commission Staff Working Paper on Development of second generation SIS II, December 2004 Progress Report, Council Doc 7964/05, 31.3.3005, SEC(2005) 338

Common Consular Instructions OJ C 313/1,16.12.2002

Common Manual on list of visa applications requiring prior consultation with the central authorities, in accordance with Article 17 (2) OJ C 313/97, 16.12.2002

Communication from the Commission to the Council and the European Parliament, Development of the Schengen Information System II, COM(2001) 720 final, 18.12.2001

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders Official Journal L 239 , 22/09/2000 P. 0019 - 0062

Convention for the Protections of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") European Treaty Series 108 - Automatic Processing of Personal Data, 28.1.1981

Council and Parliament Directive 95/46/EC OJ L 281 , 23/11/1995 P. 0031 - 0050

Council Communications SCH/Com-ex (93)9 and SCH/Com-ex (94)28 rev.) on the fight against illegal trafficking in narcotic drugs and psychotropic substances and Note from EU Presidency to Council/Mixed Committee 14790/01on violent troublemakers and persons subject to criminal investigations.

Council Conclusions JHA of 5/6.6.3 re SIS docs 10054/03; 10055/03; 5003/2003 WG

Council Decision 1999/435/EC OJ L 176, 10/07/1999 P. 0001 - 0016

Council Decision 1999/437/EC OJ L 176, 10/07/1999 P. 0031 - 0033

Council Decision 2000/365/EC OJ L 131, 01/06/2000 P. 0043 - 0047

Council Decision 2000/751/EC OJ L 303, 02/12/2000 P. 0029 - 0029

Council Decision 2004/496/EC on the conclusion of an Agreement between the European Community and the USA on the processing and transfer of PNR data by Air Carriers to the US Department of Homeland Security Bureau of Customs and Border Protection ,OJ L 183 of 20.5.2004, P83)

Council Decision 2004/512/EC OJ L 213, 15.6.2004

Council Decision 2005/211/JHA OJ L 068 , 15/03/2005 P. 0044 – 0048

Council Regulation (EC) 871/2004 OJ L 162 , 30/04/2004 P. 0029 - 0031

Council Regulation (EC) No 2424/2001 OJ L 328 , 13/12/2001 P. 0004 - 0006

Decision of the Executive Committee of 28 April 1999 on the definitive versions of the Common Manual and the Common Consular Instructions (SCH/Com-ex (99) 13) OJ L 239 22.9.2000 P. 0317 - 0404

Den Boer, Monica (2004) *Plural Governance and EU Internal Security: Chances and Limitations of Enhanced Cooperation in the Area of Freedom, Security and Justice,* Paper for ARENA, Oslo, 25.5.2004

Directive 64/221/EC OJ 056, 04.04.1964 P. 0850 - 0857

Directive 68/360/EC OJ L 257 , 19.10.1968 P. 0013 - 0016

Directive 95/46/EC OJ L 281 21.11.1995 P 0031 - 0050

Directive 2004/38/EC OJ L 229 , 29.06.2004 P. 35 – 48

Draft Council Regulation on standards for security features and biometrics on passports and travel documents, Council Doc 15139/04 LIMITE VISA 208 COMIX 714, 23.11.2004

Draft Council Resolution on security at European Council meetings and other comparable events, 30.06.2003, Council Doc. 10965/03 ENFOPOL 63 COMIX 417

German Federal Data Protection Commissioner, Annual Report 2003/2004 of the Federal Commissioner for Data Protection, www.bfd.bund.de/information/tb04_engl.pdf

Groenendijk, Kees (2004) "Reinstatement of controls at the internal borders of Europe : Why and against whom?" in *European Law Journal*, Vol.10 No. 2, March 2004, pp150 - 170

Guild, Elspeth "Désaccord aux frontières et politique des visas : les relations entre Schengen et l'Union" *Cultures et conflits* www.conflits.org/document.php?id=927

Guild, Elspeth, "Le Visa : instrument de la mise à distance des "indésirables" , *Cultures et conflits* www.conflits.org/document.php?id=933

Guiraudon, Virginie, (2001) *The EU "garbage can": Accounting for policy developments in the immigration domain,* .Paper presented at the 2001 conference of the European Community Studies Association in the panel "Immigration and the Problems of Incomplete European Integration," Madison Wisconsin, 29 May-1 June 2001, http://www.eustudies.org/GuiraudonPaper.do

Hustinx, Peter J. (2004) European Data Protection Supervisor, Speech given at Scientific Conference on New Ideas and Trends in the Field of Third Pillar and Law Enforcement Data Protection, Budapest ,1.12.2004

Joined Cases C-465/00, C-138/01 and C-109/01, Rechnungshof, Osterreichischer Rundfunk and others, Judgment of the Court, 20.5.2003 (1)

Joint Supervisory Opinion on the development of the SIS II, 19.5.2004

JSA information leaflet "Your Rights and the SIS" (undated)

JSA Opinion on the development of SIS II, SCHAC 2504/04

JSA Report Jan 2002 – Dec 2003

Letter from the Chairman to Bob Ainsworth MP, Under-Secretary of State, Home Office, Written Evidence of the House of Lords Select Committee on European Union, Schengen Information System : New Functions (Council Doc 9407/02 and 9408/02), 9.4.2003

List of authorities for the purposes of article 101(4) Schengen16023/04 SIRIS 144 COMIX 768

Moon (Unreported, November 6, 2002) (CE (F)) Conseil D'Etat (Assemblée), in comment by Roger Errera, *Public Law* 2003, SPR, 187-190

Moon (2 June 2003) Conseil D'Etat Decision n° 194295

Errera Roger (2003) Case Report on Moon (Unreported, November 6, 2002) *Public Law* 2003, SPR, 187-190

Note from Europol (Legal) issues raised during the last session of the EU Working Party SIS in relation to access to the SIS for Europol, 9323/02 LIMITE SIS 35 EUROPOL 42 COMIX 363, 28.5.2002

Note from General Secretariat on Table of hits recorded by the SIRENE bureaux for period 1

January 2002 to 31 December 2003, Council Doc 7915/04 LIMITED SIRIS 47 COMIX 226, 2.4.2004

Note from Netherlands, German, Austrian and Belgian delegations on SIRPIT (Sirene Picture Transfer) – SIRENE Procedure, Council Doc. 9450/02, LIMITE SIRENE 41 COMIX 374, 30.5.2002

Note from Presidency on SIS Database Statistics, Doc No 8621/05 SIS-TECH 38 SIRIS 38 COMIX 285, 2.6.2005

Note from Presidency on SIS II functions/open issues, Council Doc No 12573/3/04, REV3 LIMITE SIRIS 94 COMIX 566, 30.11.2004

Note from Presidency on Mandate for a technical analysis concerning the implementation of Article 1(9) of Decision 2005/211/JHA - Access to the SIS for Europol, 8874/05 SIRIS 42 SIS-TECH 47 COMIX 310

Note from Presidency on Assessment of the state of the SIS II project Council Doc 9672/05 LIMITE SIRIS 56 COMIX 366

Note from Presidency on Comments on the Commission's progress report for SIS, Council Doc 8506/05 LIMITE SIS-TECH 36 COMIX 272, 27.4.2005

Note from Presidency on JHA Council Declaration: follow up, Council Doc 11330/05

Note from Presidency on Parameters, procedures and time schedule for decision on the strategic management of SIS II, Council Doc 12888/04 LIMITE JAI 355 SIRIS 98VISA 176 COMIX 582, 4.10.2004

Note from Presidency on SIS Requirements, Council Doc. 5968/02, 5.2.2002

Note from the Chairman of the JSA to the Chairman of the Article 36 Committee, SCHAC 2502/2/02 REV 2, 11.3.2002

Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and Council concerning the VIS and the exchange of data between Member States on short stay-visas, COM(2004)835 final OJ C181/06, 23.3.2005

Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the exchange of information from criminal records, COM (2004) 664 final of 13 October 2004,13.1.2005

Opinion of the European Data Protection Supervisor on the Proposal for Council Decision (COM)(2005) 200 final, 1.5.2005

Opinion of the JSA Concerning the relation between Articles 112 and 113 Schengen Convention SCHACH 2510/1/02 REV1, 7.10.2002

Principle 5.5.ii Recommendation No. R(87) 15, adopted by the Committee of Ministers on 17.9.1987

Proposal for Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II) Council Doc. 9942/05 COM (2005) 230 Final 31.5.5

Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) Council Doc.9943/05COM (2005) 236 Final 31.5.2005

Proposed Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates COM(2005)237 final, 31.05.2005

The Prüm Convention 10900/05, LIMITE CRIMORG 65 ENFOPOL 85 MIGR 30, 7.7.2005

Recommendation from the Schengen JSA, Archiving documents after an alert has been deleted, SCHAC 2505/99 LIMITE, 11.10.1999

Regulation (EC) 45/2001 of the European Parliament and of the Council OJ L 008, 12.1.2001 P 0001 - 0022

Rekvényi v Hungary (Application no. 25390/94) ECHR, Judgment 20 May 1999

Report of the Netherlands Court of Auditors (Algemene Rekenkamer) on the National Schengen Information System 1997 http://www.rekenkamer.nl/cgi-bin/as.cgi/0282000/c/start/file=/9282400/modulesf/gxem5irq

Saas, Claire "Refus de deliverance de visa fondé sur une inscription au SIS", *Cultures et conflits* www.conflits.org/document.php?id= 917

Salter, Mark (2004) "Passports, Mobility, and Security: How smart can the border be?" *International Studies Perspectives* (2004) 5, 71–91

Sirene Manual OJ 2003/C38/01 12.2.2003

Statewatch Analysis, SIS II: fait accompli? http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf

Submission by Justice to the House of Lords European Communities Committee (Sub-Committee F) on European Databases, April 1999

Thym, Daniel: The Schengen law : a challenge for accountability in the European Union, *European Law Journal* Vol. 8 No. 2, June 2002, pp218 – 245, p242

Van Buuren, Jelle "Les tentacules du système Schengen" *Le Monde Diplomatique*, March 2003 http://monde-diplomatique.fr/2003/03/VAN_BURREN/9970

Written question No. 19/98 by Nikitas Kaklamanis to the Commission. Official Journal C 196 , 22/06/1998 P. 0107