RANKED AMONG THE WORLD'S TOP 10 THINK TANKS
CEPS Liberty and Security in Europe
CENTRE FOR EUROPEAN POLICY STUDIES

The Difficult Road to the Schengen Information System II:
The legacy of 'laboratories' and the cost for fundamental rights and the rule of law

Joanna Parkin

April 2011

Abstract

This paper seeks to understand the reasons behind the considerable complications facing the project to develop a new, second generation version of the Schengen Information System (SIS II). Despite the centrality of this large-scale EU database for immigration and border control purposes and the increasing prioritisation of security technologies within the EU's internal security strategy, the project has encountered substantial delays, an escalating budget, political crises and criticisms of the new system's potential impact on fundamental rights.

To uncover the underlying causes of these difficulties and deficiencies, the paper examines the decision-making processes that have shaped the development of SIS II over the last decade. It argues that there are strong parallels between the policy processes surrounding SIS II and decision-making under the old Schengen regime, where expert driven, security oriented and fragmented decision-making took place outside the EU framework and beyond the reach of democratic and judicial oversight. The paper contends that decision-making on SIS II undermines principles of proportionality, accountability and fundamental rights and, by extension, puts into question the political legitimacy of the EU's Area of Freedom, Security and Justice. The paper concludes with a set of policy recommendations intended to inform the future development of large-scale EU IT systems.

Research for this paper was conducted in the context of INEX, a three-year project on converging and conflicting ethical values in the internal/external security continuum in Europe. The project was funded by the Security Programme of DG Enterprise of the European Commission's Seventh Framework Research Programme and coordinated by PRIO, International Peace Research Institute in Oslo.

ISBN 978-94-6138-088-3
Available for free downloading from the CEPS website (http://www.ceps.eu)

CONTENTS

The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law

Joanna Parkin*

CEPS Paper in Liberty and Security in Europe, April 2011

Introduction

The Schengen Information System (SIS I) is one of the most important large-scale databases used for immigration and border controls in the European Union (EU.) Conceived as a tool to compensate for the insecurity implied by the lifting of EU internal borders under the Schengen regime, SIS I has become a political cornerstone of the EU's Area of Freedom, Security and Justice (AFSJ). Accordingly, the development of an upgraded, 'second generation' Schengen Information System (SIS II) to accommodate new member states and new functionalities has constituted a central priority on the EU's agenda for the past decade.

Yet despite the weight accorded to this enterprise, the SIS II project has experienced numerous setbacks and delays. The original deadline for the operational launch of SIS II in 2006 has long since elapsed, during which time the project has experienced a 500% increase in its budget, escalating tensions between member states and the European Commission and a political crisis that has placed the very viability of the project in doubt. More seriously, question marks now hang over the potential ethical and fundamental rights implications of this new EU level large-scale database, one of the prime functions of which is to record information on 'inadmissible' third country nationals, operated by police-led national law enforcement authorities.

In attempting to unravel the underlying causes of these difficulties and deficiencies, an examination of policy processes on SIS II reveals striking parallels between the evolution of this new large-scale EU database and the origins and development of the SIS I and the Schengen system itself. SIS I was forged in 'the Schengen laboratory', a project of intergovernmental cooperation widely heralded for enabling a small group of member states to advance European integration outside the EU Treaties framework in sensitive areas such as borders, security and police cooperation. Though criticised for its lack of transparency and democratic unaccountability, co-operation under Schengen has been made legitimate through its analogy with an 'experiment' that allowed a small number of countries to set a blueprint for cooperation that could be expanded to the rest of the EU (Guild, 2001).

Yet, the incorporation of the Schengen structures into the framework of the EU with the Treaty of Amsterdam in 1999 did not establish the degree of legal and institutional coherence that many had anticipated (see de Zwaan, 1998).[1] Rather it codified pre-existing legal and political

* Joanna Parkin is a research assistant in the Justice and Home Affairs section of the Centre for European Policy Studies (CEPS). This paper was drafted under the supervision of Sergio Carrera, Senior Research Fellow and Head of Section at the Justice and Home Affairs Section of CEPS. The author is grateful to Sergio Carrera, Elspeth Guild and Gloria González Fuster for their comments on the preliminary version of this paper. She would also like to thank the officials of the European Commission, Council, Parliament and the European Data Protection Supervisor (EDPS), as well as the national experts and civil servants who were interviewed for the purposes of this paper.

[1] De Zwaan anticipated that "the substitution of the former Schengen structures by the ordinary Union working methods may be regarded as a qualitative step forward. Indeed, the confusion which has arisen in

arrangements, institutionalising a high degree of complexity and fragmentation in the Area of Freedom, Security and Justice (AFSJ), reducing the transparency of decision-making, making democratic oversight more difficult and leading to deficits in judicial control (Monar, 2001; Den Boer, 2002; Stubb, 1996; Edwards and Philippart, 1999). Furthermore, the police-based networks of security and law enforcement experts that had played a central role in advancing the Europeanisation of police cooperation and forging the security-oriented logic of the Schengen system remained active in the plethora of working groups and committees that emerged within the Council framework under the former third pillar (Bigo, 1996).

This paper seeks to provide an understanding of the delays, technical difficulties and ethical deficits of SIS II by charting the genealogy of the SIS II project from its Schengen origins to the present day. It contends that, while acknowledging the technological complexities of developing a large-scale IT system for the EU, the problems encountered find their roots in the 'Schengen model' of decision-making which endures within the EU's AFSJ and of which the SIS II presents a paradigmatic example.

The paper highlights how the design and development of SIS II have been driven by a multiplicity of diverse actors, including national police experts, civil servants from national ministries of interior and specialists in security technologies, acting within highly in-transparent working structures and beyond the scrutiny of mechanisms for democratic accountability and rule of law that characterise the Community method of cooperation envisaged by the EU Treaties. It charts the ways in which a logic of (in)security, elaborated under the Schengen System, was redeployed following the events of 9/11, driving forward and shaping the policy process on SIS II. By putting the focus on the elements that have underpinned decision-making on SIS II and linking them to the difficulties and deficiencies of the new system, this paper aims to draw lessons and recommendations for improved policy strategies in the development of large scale IT systems in the EU's AFSJ.

This paper is structured in five main sections: before examining the development of SIS II, it starts by outlining the origins of the SIS, its purpose, functions and deficiencies. The second section moves into an analysis of the design and evolution of SIS II from the formal decision to commence development of the new system in 2001 to the adoption of the SIS II legal basis in 2006. It argues that emergency-driven agendas and political pressures surrounding Schengen enlargement served as an impetus for negotiations within the Council at the expense of transparency and democratic accountability. The third section charts the second phase of the development of SIS II, from 2006-2011, illustrating that the technical problems, successive delays and political crises during this period have been underscored by struggles between the Commission and a multiplicity of actors for control over the ultimate direction and ownership of the project. The fourth section complements this analysis by outlining the role of expert working groups in the governance of the SIS II project, and examining their impact on decision-making. The fifth section examines the implications of the dynamics which have driven decision making on SIS II – the emergency-driven agendas, and interventions 'from below' – for accountability, proportionality and fundamental rights in the AFSJ. The paper concludes with a preliminary set of policy recommendations for improving policy strategies in the development of large-scale IT systems in the EU's AFSJ.

1. The origins of SIS II – Schengen and SIS

The SIS owes its central importance to the EU orthodoxy that states that the abolition of internal borders required a reinforced management and surveillance of external borders controls. To

practice because of the existence of a parallel circuit of bodies and procedures, and the deficiencies inherent in that construction concerning democratic and judicial control at the European level will gradually disappear."

understand the doxa of security underpinning the role of SIS, it is necessary to examine the roots and genesis of Schengen itself.

1.1 Schengen and the emergence of an (in)security logic

The initial foundation of the Schengen area was driven by economic pressures; the result of an initiative to overcome practical obstacles to cross-border trade. The first Schengen Agreement, concluded on 14th June 1985,[2] was thus negotiated largely by ministers of transport and foreign affairs, and was primarily concerned with establishing the free circulation of goods, hardly touching upon aspects of police and security cooperation.[3] However, an envoy of the German Ministry of Interior had, during negotiations on the Schengen Agreement, inserted a reference to the effect that reduction of border controls would constitute a 'security risk' of such magnitude that compensatory measures would be needed in the long run to offset this security deficit (Bigo, 1996).

The notion of a security deficit steadily took hold among the main actors advancing Schengen, until the assumption that the opening of borders would lead to an inevitable increase in crime, in turn necessitating a strengthening of police cooperation, which became the shared belief underpinning Schengen cooperation (Jeandesboz, 2010; Faure-Atger, 2008). [4] How these security concerns gained traction and legitimacy has much to do with the presence of transnational networks of police and security professionals present in an array of working parties supporting and assisting the Schengen Executive Committee. These "clubs policiers" (Bigo, 1996, p.117) were particularly active during the negotiation of the successor to the Schengen Agreement, the 1990 Schengen Convention (CISA).[5]

During the discussions on CISA, the ministries of transport and foreign affairs were gradually marginalized; replaced at the negotiating table by the participating states' ministries of interior and justice. To assist in drafting the Convention, they relied on the input of a network of working groups consisting of experts – largely police-based – drawn from their respective ministries. Despite the diverse national backgrounds of these experts, their common interest in matters of security and shared stake in advancing police cooperation in Schengen allowed them to forge and advance a Europeanisation of internal security and law enforcement. It was at the level of these expert groups that the Convention was conceived, and compensatory security measures became fully integrated into the text of the CISA.[6] According to Bigo:

[2] Agreement 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, signed at Schengen, 14 June 1985.

[3] Of the 33 articles contained in the original Schengen Agreement, only four deal with police cooperation.

[4] It is worth noting that 12 years after the adoption of the Schengen Implementing Agreement, there is no evidence to suggest a correlation between the lifting of internal border controls and levels of insecurity in the Schengen area. In fact, crime statistics gathered by Eurostat show a steady reduction in the incidence of reported crimes in the EU over the past decade. See Eurostat statistics: http://epp.eurostat.ec.europa.eu/portal/page/portal/crime/data/database

[5] Convention Implementing the Schengen Agreement of 14 June 1985, OJ L 239, 22.09.2000.

[6] Consequently, in a Convention containing 142 articles, only a minority of articles concern free movement, with most devoted to security in the form of compensatory measures (Karanja, 2008).

> The 142 articles of the 1990 Schengen Convention are therefore above all the work of these officials sharing the same vision of problems of security and not the product of considered and rational political deliberations at the inter-governmental level (1996, p.129).[7]

Consequently, with the conclusion of the Schengen Convention the focus of the Schengen system narrowed, from promoting the free movement of goods and persons to a system primarily centered on ensuring that 'undesirables' could not gain entry to participating states (Guild, 2001; Groenendijk, 2004). Prime targets among such unwanted persons were third country nationals. The Schengen Information System, laid down in Articles 92 to 101 of CISA, became the central means to enforce the surveillance of unwanted persons.[8]

1.2 SIS I: purpose and functions

The overarching aim of the SIS, as laid down in the CISA is to maintain:

> …public order and security, including state security, and to apply the provisions of this convention relating to the movement of persons, in the territories of the contracting parties, using information transmitted by the system. (Article 93, CISA).

The system is based on a 'hit/no hit' query function which indicates whether information on a person or object exists within the system, thus alerting police officers, border guards and customs officials across the Schengen area to persons and items that may pose an immigration or security risk. The SIS is made up of a central system (C-SIS) physically located in Strasbourg and national databases (N-SIS) in each of the participating states. The exchange of additional, background information relating to the alerts in case of a 'hit' takes place through the SIRENE network of national contact points.

Since the SIS became operational in March 1995, it has gradually expanded from an initial use by seven member states (Belgium, France, Germany, Luxembourg, Netherlands, Portugal and Spain) to become fully applicable in 22 EU member states, plus Switzerland, Norway and Iceland.[9] Currently the SIS includes more than 35 million records, of which just under one million are records on persons.[10] This massive expansion in the use of the SIS has necessitated successive updates of the system: in 2001 SIS was expanded into SIS I+ in response to the inclusion of the Nordic countries (Denmark, Sweden, Finland, Norway and Iceland), and in 2007 SISone4all was put in place to manage the enlargement of the Schengen area to encompass nine of the countries that acceded to the EU in 2004 (Czech republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia).

---

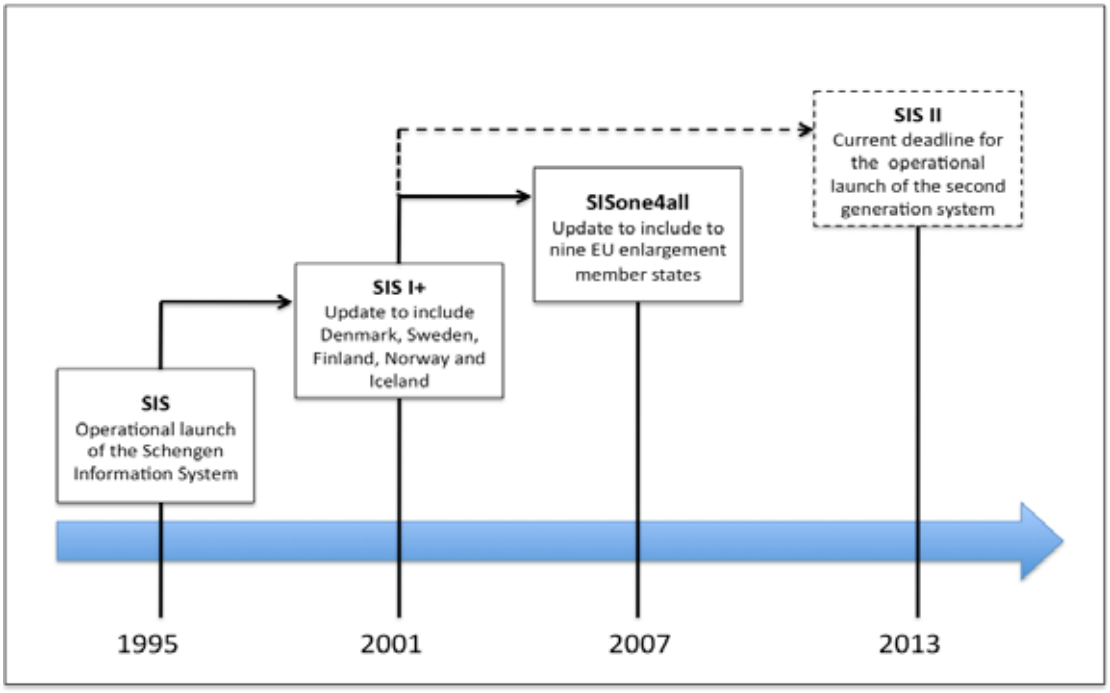
[7] *"La Convention de Schengen de 1990 de 142 articles, est donc avant tout l'œuvre de ces fonctionnaires partageant une même vision des problèmes de sécurité et non le produit réfléchi de délibérations politiques rationales à l'échelle inter-gouvernementale."*

[8] For an historical overview of the creation of Schengen and the development of SIS I, see chapters 2 and 3 of E. Brouwer, 2008.

[9] The UK and Ireland participate in the police cooperation aspects of the Schengen Convention and SIS, with the exception of alerts relating to third country nationals.

[10] Council document, Schengen Information Database Statistics 01.01.2011, 6434/1/11.

Figure 1. Chronology of the evolution of the Schengen Information System



Source: Author's elaboration.

Out of the five categories of persons for whom data may be entered in the SIS,[11] the largest category is "persons to be refused entry to the Schengen area as unwanted aliens" (Article 96, CISA).[12] Consequently, it has been suggested that while the official purpose of the SIS is to maintain 'public order and security', its main preoccupation is with policing irregular immigration (Broeders, 2007). The close association between immigration, criminality and law enforcement that has become an increasingly common feature of EU migration law and policy is crystallized within the SIS. Third country nationals are to be treated with suspicion, not as individuals who pose a specific threat, but as members of a group profiled as a risk category (Cholewinski, 2007.)

Consequences for a third country national reported in the SIS can be grave: they may be refused entry or a visa, or even detained or expelled. Due to the principle of mutual recognition, the entry ban applies not only to the member state which initially reported them but any other EU member state. It is therefore of serious concern that deficiencies regarding data quality and data protection have been identified in SIS I.

[11] The remaining five categories of alerts contained within the SIS are: persons wanted for arrest or extradition (Article 95 CISA); missing persons or persons who need to be placed under protection (Article 97 CISA); persons sought by judicial authorities in connection with criminal proceedings (Article 98 CISA); persons who are to be subject to discreet surveillance or a specific check (Article 99 CISA); and lost or stolen objects (Article 100).

[12] According to the statistics on records held in SIS from 2011, there are 716, 797 records registered under Article 96 CISA, against 31, 535 records under Article 95; 24, 350 under Article 97; 82, 676 under Article 98; and 36, 478 under Article 99. See Council document, Schengen Information Database Statistics 01.01.2011, 6434/1/11.

1.3 SIS I deficiencies regarding data protection and fundamental rights

The data protection and fundamental rights deficiencies of SIS I have been the target of sustained criticism by academics, EU bodies and civil rights organisations alike (Brouwer, 2008; Karanja, 2008; Hayes, 2008). They can be primarily broken down into three categories: first, a breach of the purpose principle enshrined in data protection law; second, problems of data quality linked to divergent national practices in entering alerts; and third, problems of access to legal remedies.

First, a central tenet of the fundamental right to the protection of personal data as defined in Article 8 of the EU Charter of Fundamental Rights is that "data must be processed fairly for specified purposes."[13] Yet the very design of the SIS contravenes this principle, as it contains both law enforcement information (e.g. persons wanted for arrest) and border control and immigration information (e.g. banned third country nationals). In theory, a boundary between these two purposes is maintained by obliging each member state to declare which of its authorities has access to which set of SIS data. In practice however, this provides little guarantee as member states are free to designate their "competent authorities" (see Geyer, 2008). The European Commission has recently acknowledged that the SIS does not comply with the principle of purpose limitation.[14]

Second, the grounds provided in the Schengen Convention for entry of third country nationals under Article 96, CISA are not sufficiently defined. Consequently, member states have adopted very different interpretations of the notion of what constitutes a risk to security and public policy (Guild, 2001; Guild and Bigo, 2002).[15] This has led to a wide variation in practices between national authorities when reporting individuals in the system, resulting in many cases of inaccurate, unlawful data entered on the SIS.

For instance, inspections by the Schengen Joint Supervisory Authority (JSA)[16] found that certain member states have entered considerably more alerts in the SIS I under Article 96 than others. Furthermore, reasons for entry differ markedly. For instance, Germany and Italy were found to be incorrectly registering under Article 96 failed asylum seekers and migrants violating immigration rules en masse.[17] Similar discrepancies were found regarding alerts entered for persons targeted for discreet surveillance (Article 99).[18] In response to these worrying findings,

---

[13] Article 8.2 of the Charter of Fundamental Rights of the European Union O.J. (2010/C 83/02), 30.03.2010.

[14] See Commission Communication on an Overview of information management in the area of freedom, security and justice, COM(2010)385, Brussels, 20.7.2010, p.22.

[15] The example of the New Zealand Greenpeace activist who was prevented from entering the Netherlands in 1998 on the basis of an SIS entry by France is a case in point. The French authorities judged that this individual represented a threat to internal national security as she had been demonstrating against France's testing of nuclear bombs. Presentation by H. Staples: Judicial Control of the EU Border: ILPA/Meijers Committee Conference: 11 & 12 May 2001, London.

[16] The Joint Supervisory Authority is an independent body established under Article 115(1) CISA and charged with supervising the technical support function of the SIS.

[17] A JSA Report of 2005 found that Italy and Germany were responsible for recording 77% of the total number of Article 96 alerts registered in 2003. Joint Supervisory Authority of Schengen, *Article 96 Inspection. Report of the Schengen Joint Supervisory Authority on an Inspection of the Use of Article 69 alerts in the Schengen Information System*, 20.06.2005.

[18] Massive discrepancies in the use of Article 99 among the participating states have been reported, with France, Italy and Spain entering tens of thousands of alerts during the course of one year and other member states, such as Ireland or Greece, entering few or none. See Joint Supervisory Authority of Schengen, *Article 99 Inspection. Report of the Schengen Joint Supervisory Authority on an Inspection of the Use of Article 99 alerts in the Schengen Information System*, 18.12.2007.

the JSA issued a comprehensive set of recommendations on article 96 alerts. However, a follow-up inspection conducted in 2010 found that only a handful of Schengen states showed improved compliance, with others demonstrating no sign of having implemented the JSA's guidelines.[19]

Third, there are obstacles hindering the ability of a third country national facing an SIS alert to exercise their fundamental right to access, correct or delete personal information held on databases. Weaknesses stem from several factors:

- Individuals are generally not informed that they have been registered in the SIS.[20] Third country nationals will often only find out about their registration when it is too late, either when being denied access at the external borders of the EU or refused a visa.
- Even when aware of their registration, the possibility for an individual to access remedies against the wrongful entry of data in SIS is subject to a diversity of procedures under national law. Some member states allow only indirect access to personal data held on the SIS, which means that individuals seeking to rectify inaccurate data on the SIS must first go through the National Data Protection Authorities. This can result in long delays for obtaining information and the degree of information ultimately provided is sometimes minimal, with little or no guidance provided regarding right to redress (Brouwer, 2008b).
- The outcome of appeal proceedings dealing with an SIS alert have been found to be widely divergent, depending on the country in which the appeal is lodged or the court considering the appeal. Moreover, some national courts have been reluctant to rule on the legitimacy of decisions taken by authorities of other member states (Brouwer, 2008b).
- The possibility to seek redress against an SIS listing is often unavailable to third country nationals, as the national legislation of member states does not always provide for legal remedies in immigration law procedures (Brouwer, 2008).

High variances in the use of the SIS are partly a reflection of the intrinsically national nature of this instrument. Each member state manages its own national systems and it is national legislation which predominantly governs the ability of individuals wrongly reported to have information corrected and seek compensation. Nevertheless, the identified weaknesses point to a clear need for a re-assessment of the rules governing the use of the SIS, in order to safeguard civil liberties and fundamental rights.

The development of SIS II would have offered the opportunity for such a re-assessment. However, data protection concerns and fundamental freedoms have not been the main factors driving its development. Rather, while the initial reasons for developing a second generation of the SIS was to allow for the integration of the ten new enlargement countries that acceded to the EU in 2004, attention quickly focused on the opportunity to add a series of new technical features and functionalities, including new categories of alerts, the storage of biometric data (photos and fingerprints) and the interlinking of alerts.[21]

The new functions planned for SIS II pose a new set of ethical questions, not least because they imply a shift in the purpose of the SIS from essentially a hit/no hit system into a much more

[19] Joint Supervisory Authority of Schengen, *Article 96. Report of the Schengen Joint Supervisory Authority on the follow up of the recommendations concerning the Use of Article 96 alerts in the Schengen Information System*, 26.11.2010.

[20] For instance, an investigation by the Dutch Ombudsman into the registration of third country nationals in the SIS found that immigrants were not properly informed of the fact that they are registered or what this registration implies and how they might contest it. See Nationale ombudsman, *Toegang verboden. Onderzoek naar de opname van vreemdelingen in het Schengen Informatie Systeem en de informatievoorziening hierover*, Rapport 2010/115. Den Haag 2010, cited in Besters and Brom, 2010.

[21] For a detailed analysis of the changes introduced by the SIS II, see Peers, 2008.

complex investigative tool.[22] In order to understand the rationale and considerations driving the introduction of these new features, and the considerations (or lack of) accorded to ethical and fundamental rights implications of the new system, it is necessary to examine the legal and political conditions that formed the backdrop for negotiations on the design of SIS II.

2. Towards the development of SIS II: 2001-2006

The incorporation of the Schengen *acquis* into the EU legal and institutional framework with the Treaty of Amsterdam in 1999 was finally expected to confer legitimacy on the Schengen regime. However, the transfer of the acquis into the EU framework was an arduous and highly politicised process which, it has been suggested, resulted not in the communitarisation of Schengen, but rather the Schengenisation of the newly established AFSJ (Zaiotti, 2011). Having agreed to split the Schengen provisions between the third and the first pillar of the former EU Treaties, drawn out negotiations surrounded the allocation of a legal basis to each provision (the so-called 'ventilation procedure'). It was broadly agreed that provisions related to free movement of persons (visas, asylum immigration) would be placed under the first pillar (Title IV of the former TEC on "visas, asylum, immigration and other policies relating to freedom of movement") governed by the community method of decision-making while the "compensatory" security measures would be placed under the third pillar (Title VI of the former TEU on "police and judicial cooperation in criminal matters") and would continue to be governed by intergovernmental procedures.[23] The legal basis for SIS I proved to be the most divisive issue due to its dual function as a tool for both law enforcement and immigration control. With the Council unable to reach a unanimous decision, SIS was placed 'provisionally' under the third pillar, with agreement left to be determined at a later stage.[24]

The uncertainty regarding the legal basis and allocation of SIS I outside the community framework had consequences for the institutional and procedural arrangements for SIS II. Indeed, decision-making on the development of SIS II (and the amendments to SIS I which had a large influence on the final scope of the second generation system) in many ways mirrored the classic Schengen model. This was manifest, firstly, in the 'experimental' and fragmented approach to policy formation, made possible by the fact that work began on the new system several years before the legislative package for SIS II was adopted in 2006. This meant that the elements usually stipulated in legislation, the system's overall purpose, functionalities and the respective roles for the EU institutions, were not defined in advance but developed in parallel with the project itself, leaving room for substantial input by national delegations and experts based in Council working groups under the third pillar.

Secondly, decisions on the scope of SIS II were, as with the Schengen Convention, shaped by a doxa of security based on the construction of new transnational 'threats' to the EU, now strengthened following the acts of political violence in New York in 2001 and Madrid in 2004. The politics of emergency surrounding 9/11 drove forward and shaped a policy process where there was no clear legal competence. It allowed member states to quickly agree on a number of functionalities for SIS II which, given their implications for fundamental rights and rule of law, would have otherwise provided points of profound controversy. How these two factors – the

[22] See the Report of the JSA of 2002-2003 in which it warned that the changes to SIS II "would result in a fundamental change to the nature of the system… the SIS II looks set to become a multi-purpose investigation tool." JSA Report, January 2002-December 2003, cited in Garside, 2005.

[23] Council Decision 1999/435/EC concerning the definition of the Schengen *acquis* for the purpose of determining, in conformity with the relevant provisions of the EC and EU Treaties, the legal basis for each of the provisions or decisions which constitute the *acquis*, OJ L176, 10.7.1999.

[24] For a detailed discussion of the incorporation of the Schengen *aquis* into the EU framework and the problematic place of the SIS, see S. Karanja, 2008 or R Zaiotti, 2011.

institutional setting and the political pressures of 9/11 – framed the design of the SIS II are further explored below.

2.1 Laying the groundwork for a flexible system

Negotiations on the creation of a new version of SIS had been underway since 1996; however they intensified at the turn of the century in anticipation of the 2004 EU enlargement. The need to integrate the ten new accession states in Schengen would require a new version of the SIS, as the original did not allow for the participation of more than 18 countries. Unable to agree which member state should take overall responsibility for managing the development of the new system, the Commission was requested to assume this role. In December 2001, first and third pillar legislation was adopted conferring project management powers on the European Commission,[25] with agreement that the project would be financed from the EU budget.[26] It has been suggested during the course of interviews that the Commission was initially reluctant to embark on such a large project, without first establishing the appropriate legislative instruments and respective institutional framework.[27] However, these concerns were overridden by considerable political pressure from the member states to begin development as soon as possible and to deliver the finalised system by 2006.

Although the 2001 legislation on the development of SIS II did not explicitly refer to extended functions, from the outset negotiations began on the possible new functionalities that the SIS II could include. Experts present within the Council working groups had already made progress on preparatory work for SIS II, with the SIS and SIRENE working groups having drafted a list of possible new features.[28] In June 2002, the Ecofin Council approved conclusions on the new requirements for SIS II which referred to the inclusion of biometric data, the possibility of interlinking alerts and the addition of new categories of data. These changes were agreed "with a view to ensuring greater effectiveness in combating terrorism."[29]

In 2003, the Commission noted that "demands on new functions and new information types are continuously being discussed within the decision-making bodies. In due time, some or all of these have to be included in the features of the SIS II."[30] In anticipation of the outcome of these negotiations, and so as not to delay the development of the system, the Commission proposed to build a flexible technological architecture that would be capable of incorporating a range of potential functionalities (See Besters and Brom, 2010). This flexible system would, in the Commission's view, enable the integration of new functions which "in the light of events such as those of 11 September, would not require too long implementation time frames in the future."[31] The implication was that whenever the Council agreed on the introduction of a new function and arranged the legal framework accordingly, the function could be updated

[25] Regulation 2001/2424 and Decision 2001/886 on the development of the second generation Schengen Information System (SIS II), OJ L 328, 13.12.2001.

[26] Report of the meeting 9118/01 (Presse 203).

[27] See these concerns also reflected in the Commission Communication on the Development of the Schengen Information System II, COM(2001) 720 final, 18.12.2001, pp.13-14.

[28] Document SN 2728/01, outlining the strategic technical requirements on a new infrastructure for SIS; and the SIS-TECH 32 outlining the technical implications of the new functions which are currently under discussion at Council level.

[29] Council conclusions 10089/02 (Presse 181), Madrid, 20 June 2002.

[30] Commission Communication on the development of the Schengen Information System II, and possible synergies with a future Visa Information System (VIS), COM (2003) 771 final, 11.12.2003.

[31] Commission staff working document on the development of the second generation Schengen Information System, 2002 Progress Report, 18.02.2003, SEC (2003) 206.

immediately. Consequently, it was agreed at the June 2003 JHA Council meeting[32] to instruct the IT contractors developing the SIS II (the French company HP Steria) to incorporate in its technical design the possibility to add 'new functions', despite the fact that these had yet to be agreed upon at political level.[33]

2.2 The politics of emergency in expanding the scope of SIS II

Directly following the 9/11 events, the EU institutions and national governments volunteered a number of measures and proposals in the area of Justice and Home Affairs designed to strengthen 'the fight against terrorism' (see Brouwer, 2003; Brouwer, Catz and Guild, 2003). While many of these measures were presented as brand new, developed in the face of the new terrorist threat, in reality they had been in the pipeline for some time and the interest was primarily to exploit the political momentum provided by contemporary events to force through a set of highly contested technical security measures (Bigo and Carrera, 2004; Mitsilegas, 2007). In 2002, Statewatch commented on:

> an avalanche of new measures, new practices, new databases and new ad hoc unaccountable groups, most of which have very little to do with countering terrorism but rather concern crime, the targeting of refugees, asylum seekers, the resident migration population, and protests and protestors… (Bunyan, 2002).

A succession of proposals relating to the use of the SIS I and SIS II were forwarded by national governments during this period, several of which were subsequently agreed and adopted. As with wider instruments proposed under the EU's anti-terrorist policy, the implications of these measures for civil liberties and fundamental rights largely escaped scrutiny, due to the highly opaque decision-making procedures under the former EU third pillar. Negotiations took place in Council working groups, often with a raised level of confidentiality, and decisions were taken in Council meetings with no democratic or judicial oversight.

A selection of the main changes agreed by the member states during this period are set out below. Some of these proposals were considered too urgent to wait until the new system was in place and were put into operation in the first version of the SIS, while others were gradually integrated into the draft texts on SIS II. For instance the German delegation proposed a range of far-reaching measures in September 2001, which included extending access to the SIS for Europol, national public prosecutors offices and immigration and asylum authorities.[34] The possibility of extending access to the SIS beyond the police, customs and border control authorities (and visa and immigration authorities for immigration data) to agencies such as Europol and Eurojust had been advocated by the German government since the end of the 1990s. These discussions received new impetus after September 11, and at the JHA Council meeting of 19 December 2002 it was agreed that Europol and Eurojust should, in principle, have access to the SIS.[35] The details of how this access would be implemented in practice were left to be determined at a later stage. It is worth noting that a parallel proposal was forwarded by the UK delegation to also extend access for internal security and intelligence services. While this proposal failed to meet with a formal agreement, it has been suggested that an informal decision was nevertheless taken at working party level which led to access being granted to security and intelligence services at national level without a legal basis (Hayes, 2004).

---

[32] Conclusions of the JHA Council meeting of 5-6 June 2003, No. 9845/03 (Presse 150).

[33] While this paper acknowledges the role that private companies play in driving the policy agenda relating to the EU's security-related technical systems, it is not a primary focus of this paper. For further discussion, see Bigo and Jeandesboz, 2010.

[34] Meeting document, *German delegation proposal for a Council statement*, SN 4038/01, 27 September 2001, (available at: http://www.statewatch.org/news/2001/nov/sn4038.pdf).

[35] Conclusions of the JHA Council of 19 December 2002, No. 5691/02.

In early 2002, the Italian delegation proposed to report in the SIS persons on the UN terrorist lists established by the UN Sanctions Committee of Afghanistan. Although this proposal was supported and developed by the Spanish Presidency, it was never formally adopted.[36] Nevertheless, an informal agreement was taken between the Schengen states by which the German authorities would enter such persons in the SIS on behalf of the other member states (Brouwer, 2008).[37] Subsequently, a new provision was included in the SIS II Regulation by which a third country national listed on a UN terrorist list may be registered in the SIS II for purposes of refusal of entry or residence.[38]

In 2004 and 2005, two new legislative instruments were adopted on extending the use of the current SIS, based on a set of proposals forwarded by the Spanish government. *Regulation 871/2004* and *Decision 2005/211 concerning the introduction of some new functions for the Schengen Information System including in the fight against terrorism*[39] introduced a number of changes, among the most important of which was access to SIS for Europol and Eurojust (giving a legal basis to the decision taken in 2003); access by national judicial authorities to the SIS; and access by visa and immigration authorities to information on stolen identity documents.

The use of biometric information for the management of borders and the fight against crime also gained ground in the period following September 11 (Baldaccini, 2008), driven in part by the special efforts of certain member states, namely Germany and France, to push the use of biometric identification at EU level (Liberatore, 2007). In June 2003, the JHA Council agreed that SIS II should allow for the storage and transfer of biometric data.[40] A small group of member states also began exchanging photographs and fingerprints to supplement the exchange of SIS information (Brouwer, 2007). Although this exercise was initially voluntary, the project was later extended – through a recommendation agreed at the June 2006 JHA Council on the basis of an Italian proposal – to encompass other Schengen countries.[41]

2.3 The adoption of the SIS II legal basis

The wish list drawn up by the Council on future functionalities for the SIS II, as well as the changes to the SIS I, were all first adopted in the form of binding Council conclusions, meaning there was no possibility for consultation by the European or national parliaments, nor with the Schengen Joint Supervisory Body on data protection. The opportunity for an open and democratic debate came only in 2005, when the Commission finally presented legislative proposals on SIS II. This signified a turning point whereby decision-making on SIS II was removed from the exclusive control of member states and the Commission's competence in shaping the substantive aspects of the final system was increased. However, suggestions that member states had requested to participate in the drafting of the legislative proposals on SIS II

[36] Lack of adoption was likely related to difficulties of establishing a legal basis for this decision under the third pillar, the UN terror lists having already proved highly problematic under the second pillar.

[37] See confirmation of this informal agreement in note 7783/06, 7 April 2006.

[38] Article 26 of the Council Regulation 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) – establishment of the SIS/VIS Committee OJ L 381/4, 28.12.2006.

[39] Council regulation No 871/2004 concerning the introduction of some new functions for the Schengen Information System including in the fight against terrorism, OJ L 162/29, 30.04.2004; Council decision 2005/211/JHA concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 68/44, 15.03.2005.

[40] Council conclusions 9845/03 (Presse 150) 5-6 June 2003.

[41] Council conclusions 9696/1/06 of 10 June 2006.

(a request refused by the Commission) indicate that national actors were not quite ready to relinquish control over this security tool.[42]

The legislative package for SIS II presented by the Commission on 31 May 2005 comprised three instruments: a regulation and a decision addressing the establishment, operation and use of the system for immigration and policing and criminal law purposes respectively,[43] and a second regulation giving vehicle registration authorities access to the SIS II.[44] The Regulations were adopted in December 2006,[45] and the third pillar decision adopted in June 2007.[46] The timing of the proposals was not incidental, but followed the Council Decision of 2004, which expanded co-decision to all the fields of JHA included in the EC First Pillar, except for legal migration.[47] As the proposed legislation was subject to the co-decision procedure, they provided the first formal opportunity for the European Parliament to participate in the decision-making process on SIS II. It is not by chance that this was also the first point at which data protection and fundamental rights implications of the new system were given proper consideration. However, the scope of the Parliament's influence was to some extent constrained.

A considerable degree of haste surrounded the proposal and adoption of the legislation in view of the fact that SIS II needed to be operational by the autumn of 2007 in time for the integration of the ten new accession states and the enlargement of the Schengen area. This political urgency has been linked to the unclear nature of many provisions in the Commission's original proposals, the lack of an explanatory memorandum attached to the draft legislation and the absence of an impact assessment on the implications of the new system (Peers, 2008; House of Lords, 2007).

The Commission has argued that since the first generation of the SIS was already in operation, SIS II would only imply a change of legal base and therefore an impact assessment would not be necessary.[48] Given the substantial budgetary investment of SIS II and the fundamental rights

[42] Interviews conducted with participants, February 2011.

[43] Proposal for a regulation of the European Parliament and the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) COM(2005)236 final, 31.05.2005; Proposal for a decision of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II)COM(2005) 230 final.

[44] Proposal for a regulation of the European Parliament and 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.

[45] Regulation 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) – establishment of the SIS/VIS Committee OJ L 381/4, 28.12.2006; Regulation 1986/2006 of the regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates.

[46] Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) OJ L 205/63, 7.8.2007.

[47] Article 67 of the EC Treaty foresaw that five years after the Amsterdam Treaty entered into force (1 May 1999), the Council would take a decision providing for all or parts of the areas covered by Title IV (Visas, Asylum, Immigration and other Policies related to Free Movement of Persons) to be governed by the co-decision procedure (Art. 251 EC Treaties) and QMV voting. Following that official call for action, the Council Decision 2004/927 of December 2004 indeed provides for the extension of co-decision to all the fields of JHA included in the EC First Pillar, except for the case of legal migration. See Council Decision 2004/927/EC of 22 December 2004 providing for certain areas covered by Title IV of Part Three of the Treaty establishing the European Community to be governed by the procedure set out in Art. 251 of that Treaty, OJ L 396/45.

[48] In written evidence to the House of Lords the Commission claimed "the underlying rationale and nature of the system [SIS II] will remain the same as the current SIS. An impact assessment and public consultation were, therefore, not necessary." See House of Lords (2007) *Schengen Information System II*

implications of its new functionalities, the Commission's justification has sparked criticism from several quarters.[49]

In June 2006 the Council finished its internal debate on the legislation, during which time the Austrian Presidency had significantly re-drafted the Commission's proposals and re-introduced much of the wording from the original Schengen Convention (Peers, 2008; Brouwer, 2008).[50] In doing so, the Council deleted the Commission's attempts to amend the existing SIS rules to harmonise the grounds for entry, remove family members of EU citizens from database, to alter the rules concerning access by authorities and to take over the final management of the system once operational.

Typically, under co-decision procedure, the European Parliament would then have had significant powers to amend the legislation. However, it accepted the very tight calendar presented by the Council and the Commission and consequently agreed to conduct negotiations on the proposals through the closed-door 'trialogue procedure'. This excluded the possibility for democratic debate. Instead a compromise document was presented and the whole SIS II package was adopted at first reading on 25 October 2006.[51] Despite these constraints, the European Parliament did manage to negotiate several important amendments to the Council's version of the proposals, including the insertion of key safeguards for data protection. It also succeeded in inserting a provision on the future establishment of a management authority charged with the operational management of the central SIS II and for the security, supervision and coordination of relations between member states and the provider. However, in many respects the scope for genuine debate and room for manoeuvre on the proposals was precluded by the fact that the Council had already decided on the key functions of SIS II without any democratic consultation, leading some commentators to label them "a sham" (Peers, 2008).

3. Difficulties and delays in the development of SIS II: 2006-2010

In spite of the fast-track procedure used to adopt the legislative package in 2006, it soon became apparent that the timetable presented by the Council and the Commission to have SIS II online by mid-2007 was unrealistic. Concerns to this effect had been signalled as early as June 2005, in a note from the Luxembourg Presidency in which national technical experts attempted to correct the "impression at the political level that everything is going all right and on schedule, whereas in their opinion, this is not the case."[52] Consequently it became clear that SIS II would not be on stream in time for the accession of the new member states to the Schengen area.

3.1 Schengen enlargement and SISone4ALL

The political implications of delaying accession of the new member states to Schengen were considerable: expectations among the citizens of the accession countries that they would join by October 2007 were running high. The new member states were exerting pressure for compliance with this timetable and succeeded in securing confirmation of the October 2007 accession date

---

(SIS II): Report with Evidence, 9th Report of Session 2006-2007, European Union Committee, Stationery Office, London, p.15.

[49] Among them the UK House of Lords, which concluded: "It is unacceptable for a project with such cost and resource implications to be developed without a prior full impact assessment and a full legislative explanatory memorandum." Ibid.

[50] See the Austrian Presidency's re-drafted proposal, Council document no. 5709/06, 27 January 2006.

[51] European Parliament legislative resolution on the proposal for a Council Decision and Regulation on the establishment, operation and use of the second generation Schengen information System (SIS II), adopted on 25 October 2006.

[52] Council note 9672/05: Assessment of the state of the SIS II project, 2.06.2005.

in the conclusions of the European Council of June 2006 (Bertozzi, 2008).[53] To minimise the delay in lifting the EU's internal border controls, the Portuguese delegation to the SIS TECH Council Working Party began looking in the summer of 2006 at alternative options and came forward with a proposal for a new project called "SISone4all." This solution, based on a clone of Portugal's national system and developed by experts from Portugal's Border and Foreigners Service, relied upon extending the current version of the SIS to enable access by the new member states.[54]

Despite the misgivings of several member states and the Commission regarding the additional delays this solution would have on the SIS II timetable, as well as the increased risks it implied for the migration phase of the SIS II project,[55] the perseverance of the Portuguese coupled with the mounting political pressure of the new member states eventually secured agreement on SISone4ALL among the Schengen states in December 2006.[56] A new date was set for Schengen enlargement, and nine new member states (all except Cyprus, Romania and Bulgaria) acceded on 21 December 2007. As for SIS II, the Commission set a new date for the operational launch of SIS II from December 2008.[57]

3.2 Testing failures

The new schedule for SIS II proved optimistic, however, as the failure of a series of crucial tests in 2008 sparked a two-year crisis phase in the project.

The test phase of the central system was completed between July and December 2007.[58] However, a series of complications arose when the central unit was tested under operational conditions by a limited number of member states. The most serious problems concerned data consistency between the central and national systems but there were also weaknesses in the performance, stability and robustness of the overall system. The handling of alerts took much longer than foreseen and there were major errors in the transmission of alerts between the central and national systems, with some messages going missing and others being duplicated.[59]

The failure of these tests put the technical feasibility of SIS II into question and during this period overall confidence in the project began to stall. While there had been a loss of political momentum following the Schengen enlargement, this was now exacerbated by a growing disenchantment with the system's progress and several member states expressed their reluctance to invest more money and resources in a project whose outcome was appearing increasingly uncertain. Under the Slovenian Presidency, the JHA Council of February 2008 re-scheduled launch of SIS II for September 2009.[60] It also conceded that "a simple re-scheduling exercise

[53] The European Council of June 2006 called on the Council, Commission and member states to "take all necessary measures to allow the abolition of controls at internal borders as soon as possible, provided all requirements to apply the Schengen *acquis* have been fulfilled and after the Schengen Information System II (SIS II) has become operational in 2007."

[54] See the feasibility study conducted by the Portuguese Border and Foreigners Service and submitted the Council, 13540/06, 12 October 2006.

[55] See the note of the SIS II Task Force "Analysis of the impact of SISone4ALL on the SIS1+ and SIS II projects" 14773/06, 20.11.2006.

[56] See the conclusions of the JHA Council of 2-3 December 2006.

[57] See the press release of the JHA Council of 15 February 2007 and 19-20 April 2007.

[58] Commission staff working document, Annex to the report from the Commission on the development of the second generation Schengen Information System (SIS II) – Progress Report July – December 2007, SEC(2008) 552, Brussels, 7.5.2008.

[59] Commission report on the Development of the Second Generation Schengen Information System (SIS II): Progress Report July 2008 – December 2008 COM(2009) 133 final, 24.3.2009.

[60] Conclusions of the JHA Council of 28 February 2008, 6796/08 (Presse 48).

will not guarantee the completion of SIS II."[61] Realising that the future of the SIS II project hung in the balance, a ministerial level group composed of those member states most in favour of pushing forward SIS II development, the "Friends of SIS II" was created in a bid to inject momentum and a stronger political steer, with the formal role of monitoring progress in other member states.[62]

The success of this informal group was muted, however, as testing during 2008 encountered further technical difficulties and trust in SIS II and in the Commission's management of the SIS II project was further eroded. A small group of member states, led by Germany, France and Austria, set up a series of informal meetings between their national technical experts. Sceptical about the feasibility of SIS II but keen to have a system with the new functionalities that SIS II implied, they began to examine alternative scenarios and drew up a new solution based on using the technical architecture of the current SIS but with the addition of the new functionalities. The experts involved in the design of the alternative scenario (known also as SIS 1+ evolution or SIS 1+RE) succeeded in having the proposed solution elaborated and developed in the SIS TECH working group of the Council. In February 2009, the JHA Council requested a study be completed to make an in-depth comparison of the SIS II and the SIS 1+RE systems.[63] It also agreed on a crisis plan for the analysis and repair of the fundamental flaws in SIS II and created a Global Programme Management Board to improve coordination between national experts and the Commission.

The results of the comparison report were presented ahead of the Justice and Home Affairs Council meeting in June 2009. The meeting was to prove decisive for the future of SIS II with member states asked to determine whether to continue developing the new system as foreseen or to discontinue the SIS II project and switch to SIS 1+RE. Ultimately, the majority of member states, with the exception of France, Germany and Austria, agreed on the former. Although the comparison study found that the alternative scenario could deliver the same functionalities,[64] there was and remains a considerable degree of uncertainty regarding how to make such a system work, amid suggestions by experts that doing so would imply a significant financial investment as well as a good deal of risk. Member states also considered that they had invested too much time and resources in the original SIS II project to abandon it at such a late stage. Nevertheless, the Council agreed, at the insistence of France, Germany and Austria, to retain SIS1+RE as a fall back option,[65] and imposed on the Commission two 'milestone tests' for SIS II.[66] Should the SIS II fail to pass the milestone tests, the project will be cancelled and development will transfer to SIS 1+RE.

Preparations for this contingency plan got underway when the French authorities launched a call for tender on 1 April 2009 for the development of SIS 1+RE. The tender was subsequently awarded to the French company ATOS, the same contractor responsible for developing SIS I. Indeed, there is an understanding that should the contingency plan for SIS1+RE be activated, the member states (namely France) would be responsible for the technical development of the

---

[61] Note from the Slovenian Presidency prepared for the Informal JHA Council on 25/26 January 2008 on *Schengen Information System II*.

[62] Conclusions of the JHA Council of 28 February 2008, 6796/08 (Presse 48).

[63] Conclusions of the Justice and Home Affairs Council meeting on SIS II of 26-27 February 2009.

[64] Report on the further direction of SIS II of 20 May 2009, No. 10005/09.

[65] France was requested to launch a conditional call for tender in the spring of 2009 to develop the SIS +RE, which was awarded to the same contractor which developed SIS I, the French company ATOS. However, since the contractual deadline for the option to start developing SIS 1+RE expired in the summer of 2010, progress on the alternative solution has now been frozen.

[66] Conclusions of the Justice and Home Affairs Council meeting on the further direction of SIS II of 4 June 2009.

alternative system. While SIS1+RE would eventually be integrated with the SIS II legal instruments, its technical development would be back in the hands of the member states and the Commission would lose ownership of the project. The Council's comparison report between the two scenarios thus states that:

> Prior to its integration into the SIS II legal framework, should SIS 1+RE be developed on the basis of the Schengen Convention as amended, including its joint financing…current structures dealing with the SIS 1+ project should in principle be maintained.[67]

According to a footnote of the same report, the Austrian and German delegations had requested that an option be included:

> …which would consist of the development of *new* SIS II functionalities by the Member States under the Schengen Convention. Once the new functionalities would be ready to be put into operation, the SIS II legal instruments would start to apply to the member states after a Council decision… [emphasis added].

This request was turned down. Nevertheless, it serves to highlight the extent to which the SIS1+RE represents not only a direct political challenge to the Commission, and the Commission's capacity to manage large-scale EU IT projects, but an attempt to step back to the inter-governmental model of cooperation.

Whether recourse to the SIS1+RE alternative scenario will be required is currently uncertain. The first milestone test of SIS II took place in January 2010, with mixed results. The large majority of the technical experts in the GPMB and the SIS II Task Force announced the test inconclusive and the test was re-run in March 2010.[68] This time a majority of the member states in the various expert groups announced the tests "passed" (with the exception of the experts from Austria, France and Germany). Germany and Austria subsequently launched a scathing attack on the Commission in a note to the Council of June 2010, in which the two member states directed a string of criticisms towards a series of technical and financial decisions taken by the Commission relating to the project.[69]

The second milestone test is scheduled for the end of 2011 with the SIS II programmed to go on stream in early 2013.[70] It is open to question as to whether this new deadline for the operational launch of SIS II can be respected. From the interviews conducted it emerged that the readiness of national systems could now be problematic, given that the majority of member states froze the development of their national systems during the crisis period of 2008 and 2009. Furthermore, the external contractors developing the SIS II are obliged to implement an overhaul of the system's hardware, which, given the time lapse since the start of the project, is now outdated. This is accompanied by a substantial change to the system's software and updates to the technical specifications to integrate changes to the system's capacity and performance,[71] all of which will require a renewed series of tests. Naturally, these delays, updates and re-tests imply increased project costs, on top of the already considerable financial resources invested in the SIS II project (see section 5.2. below). Yet despite the increasing funds invested in the SIS

[67] Report on the further direction of SIS II of 20 May 2009, No. 10005/09, p.49.

[68] Results of milestone tests must be jointly validated by the Commission jointly with the Global Programme Management Board and the SIS II Task Force. See Conclusions of the Justice and Home Affairs Council meeting on the further direction of SIS II of 4 June 2009.

[69] Council note from the Austrian and German delegations on the further direction of SIS II, no. 10833/10 of 7 June 2010.

[70] Commission staff working document, Report on the global schedule and budget for the entry into operation of the second generation Schengen Information System (SIS II), SEC(2010) 1138 final, Brussels, 21.09.2010.

[71] Ibid.

II, there is still no firm guarantee that the system will be operational in the near future or indeed at all.

3.3 Identifying reasons for the delays and technical deficiencies of SIS II

How do we understand the series of delays and technical problems afflicting the development of SIS II? Certain unforeseeable challenges have played their part. For instance, the Commission was forced to put the project on hold for several months in 2005 as a result of a decision by the Court of First Instance on a legal challenge mounted by an unsuccessful tenderer.[72] Moreover, the Commission has experienced recurring problems regarding the underperformance of the external company responsible for developing the central unit of SIS II. Nevertheless, there are several structural factors at work which, it will be argued, have played a serious part in hindering the progress of this project:

First, the fact that SIS II was under development for five years without a legal basis sowed the seeds for the technical problems which emerged at a later stage. The early decision to develop an expansive and flexible SIS II architecture in order to pre-empt the outcome of negotiations on SIS II has undoubtedly increased the technical complexity of the project. Furthermore, the decision to start work on the system before having clarified its exact functions and features, as a result of the enormous pressure placed on the Commission to speed up the launch of the technical development of the system, has been a complicating factor. From the interviews conducted it emerged that the vague nature of decisions in Council conclusions meant that the original tender specifications were subsequently lacking in detail. As a result, the legislative instruments governing SIS II, when finally adopted in 2006, did not fully correspond with the original technical specifications delivered to the external contractors. This necessitated a revision of the contract, a re-design of the technical specifications and delays in the system's development. In addition, a series of subsequent technical changes have been requested by member states experts since 2006, to the extent that an advisory group, the Change Management Board, was specifically created to manage these demands (see section 4 and Annex 1). These requests have also necessitated repeated updates of the technical specifications and amendments to the contract.[73]

Second, the Commission and Council set an unrealistic timetable for the system's entry into operation, driven by the need to have SIS II on stream in time to allow for the integration of new member states into Schengen by 2006. The political unwillingness to recognise this overambitious calendar had wider implications for the direction of the project, for instance in the adoption of the intermediary solution SISOne4All. It also contributed to the rising levels of dissatisfaction with the Commission's project management performance.

Third, the SIS II project has been marked by fragmented decision-making and increasing interventions from the Council and member states, amid criticisms of the Commission's alleged inability to manage the SIS II project. For instance, interventions such as the proposal of the alternative scenario, SIS1+RE, and the imposition of the milestone tests, will not have contributed to smooth the development process. It has been suggested during the course of interviews that the procedures and working practices of a legislative body such as the European

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

[73] Between 2003 and 2010 there have been five different contracts between the Commission and the external IT company developing SIS II (the latest agreed on September 2010). See also the Commission report of 2010 which states that: "a key challenge in the development of the SIS II project has been the continuous evolution of the system's basic technical assumptions and requirements, which had an impact on the final layout of the SIS II legal basis (adopted 4 years into the project) and, implicitly, on the contractual implementation" in Report on the global schedule and budget for the entry into operation of the second generation Schengen Information System (SIS II) SEC(2010) 1138 final, 21.09.2010.

Commission are ill suited to the demands of developing a large-scale EU database, with its rapidly evolving technical demands. Furthermore, member states contend that the Commission excluded them from the early stages of the project's technical development, failing to recognise that they were key stakeholders in the process and disregarding the input of national experts. These criticisms may be well-founded. On the other hand, one must question the efficiency of a system where the authority of the project manager is repeatedly challenged by a multiplicity of managers in the form of IT and security experts drawn from national ministries of interior, private contractors, and national civil servants, often with diverging views and their own interests and objectives at stake. It has been noted that the most interventionist member states are the same core group who had been in the avant-garde of developing the first Schengen Information System. It appears that the sense of ownership over the Schengen Information System I endures within the SIS II project, manifesting in the difficulties experienced by member states to adapt their working methods on SIS II to the community framework.

Indeed, this thesis is confirmed when one examines the highly complex decision-making structures that have emerged within the EU level governance framework of the SIS II project.

4. Fragmented decision-making: Expert groups and competition for control of the SIS II project

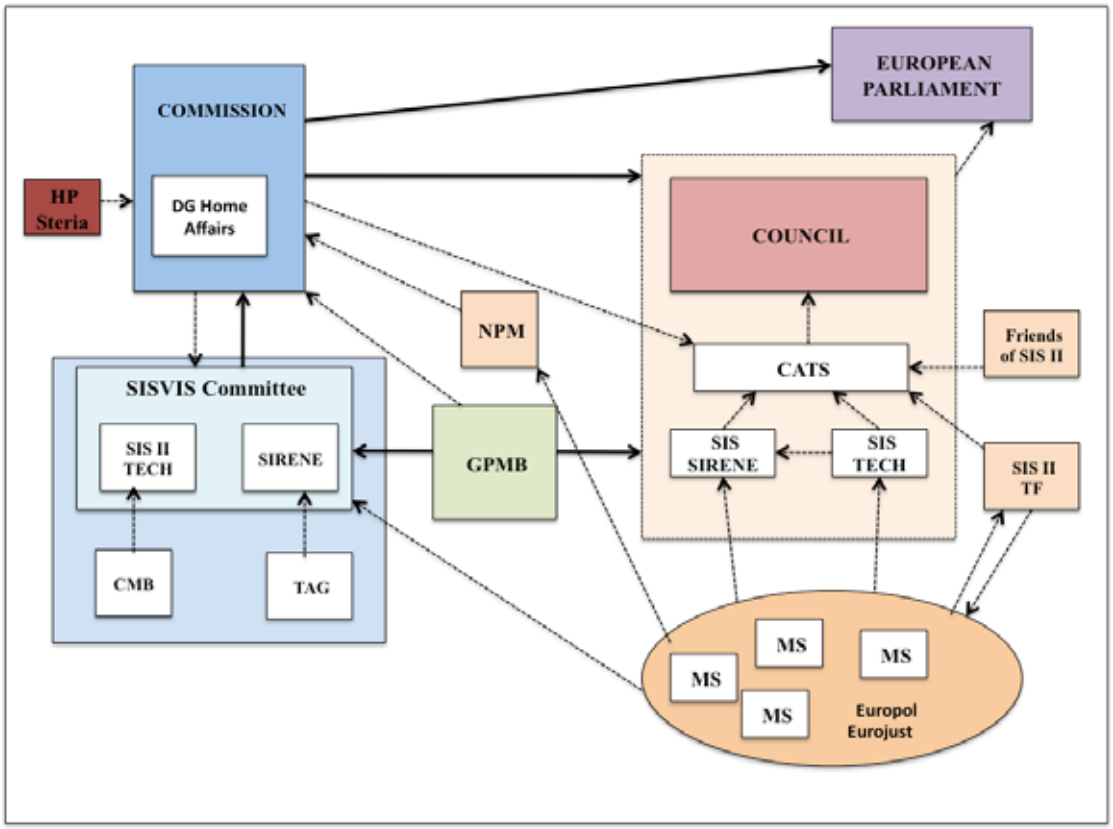
During the past decade, a complex arrangement of groups, committees, boards and task forces have emerged within the governance framework of SIS II. These groups consist of members of police boards, national technical experts, civil servants representing national ministries of interior and security bodies, and provide a platform on which a network of expertise has been constructed on SIS II. The structure and place of different groups is represented in Figure 2 below. The diagram demonstrates the channels by which knowledge and expertise 'from below' feeds into the decision-making procedures of the institutional actors, particularly the Commission and the Council. Despite the European Commission's competence for overall project management, these working structures have enabled a multiplicity of actors to gain influence over the new system's design and development, causing a fragmentation and dispersion of decision-making on SIS II.

There are currently at least 12 bodies which provide a platform for expert, inter-governmental cooperation on SIS II. These include the formal working groups active within the Council framework, of which the most important are the Article 36 Committee (CATS), and the SIS-TECH and SIS-SIRENE working parties. There are also several groups which play an active role within the Commission's comitology procedure,[74] including the SISVIS committee, which includes the sub-groups SIS II TECH and SIRENE, as well as the advisory bodies, the Change Management Board (CMB) and the Test Advisory Group (TAG). The work of the SISVIS is further complemented by regular, informal meeting at EU level of project managers responsible for the development of national systems (for a full overview of the EU level expert groups on SIS II, their roles and composition, see Annex 1).[75]

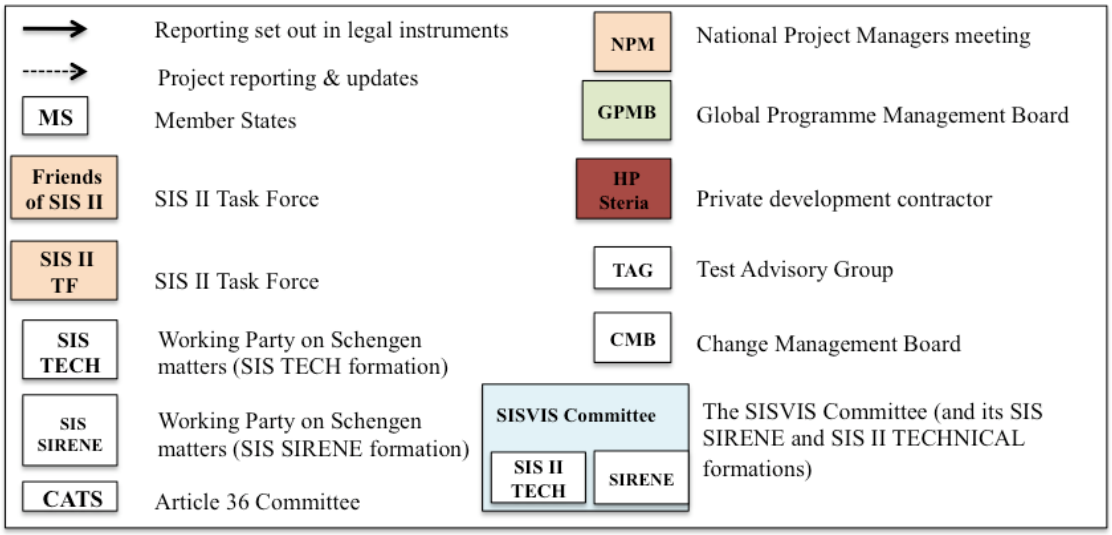
[74] For an overview of the Commission's Comitology procedure and criticisms linked to lack of transparency, and accountability and openness, see P. Craig and G. De Burca (2008) and J. Weiler (1999).

[75] The Article 36 Committee (CATS) is a formal Council working group that coordinates the working groups in the field of police and judicial cooperation; the Working Party on Schengen matters (SIS-TECH formation and SIS SIRENE formation) monitors and advises the functioning of SIS and the Sirene system respectively; the SISVIS committee (and its SIS SIRENE and SIS II TECHNICAL formations) assist the Commission in taking specific decisions relating to SIS II under the comitology procedure; the Change Management Board (CMB) is an advisory working group that examines requests for changes to the technical specifications; the Test Advisory Group (TAG) advises the SISVIS committee on tests and their

Figure 2. Diagram of the EU level governance framework on SIS II



Source: Author's elaboration



validation; the National Project Managers meeting groups the project managers from each participating state to discuss the progress of SIS II. For further details, see Annex 1.

In addition, a set of informal groupings have emerged at various stages of the SIS II project. These groups are characterised by a lack of legal basis, an unclear mandate, weak coordination and restricted participation. Though ostensibly working at the technical level, or with the purpose of exchanging good practices between the member states' national experts, they have provided an important steer to the direction of the SIS II project, [76] and offered a platform for more intensive levels of cooperation between certain member states. This has led to differentiation and, it could be argued, has further exacerbated the complications of developing SIS II.

4.1 SIS II Task Force, the Friends of SIS II and the Global Programme Management Board

Three informal groups in particular – the SIS II Task Force, the Friends of SIS II, and the Global Programme Management Board (GPMB) – have played a role at different stages of the project since 2006. They were all created at key crisis points during the project's development, and their materialisation testifies to the growing dissatisfaction and mistrust over the Commission's handling of SIS II's development. They are not the only informal groupings to have emerged at different points during the project's history, and during the course of interviews it emerged that other semi-secret arrangements between various configurations of member states have been established with the aim of exploiting mutual interests relating to SIS II. However, the SIS II Task Force, the Friends of SIS II and the Global Programme Management Board are the only groups to have been integrated into the governance framework on SIS II. They reflect a political compromise, a means of involving the member state representatives and national police experts more closely in decision-making processes, and may be seen as tangible manifestations of the struggles for control of the SIS II project. The activities of these groups are highly non-transparent and uncovering information about their membership and agendas has proved difficult.

The **SIS II Task Force** was set up during the crisis that surrounded preparations for the 2007 enlargement of the Schengen area. The group was informally established by the conclusions of the JHA Council of October 2006 in which member states agreed:

> … to set up an informal Task Force, consisting of experts seconded by *interested member states*, to assist the work of the Council, in cooperation with the Commission, on the management and coordination of the SIS II project, including the state of preparedness of all Member States. The Council invites all the stakeholders in the SIS II project to cooperate fully with the Task Force." [Emphasis added].

The group meets in the margins of comitology meetings convened by the Commission; however the Commission does not participate in the SIS II Task Force meetings. The group has no official chair, and participation is organised on a voluntary basis, although the number of member states that may participate is restricted in order to ensure the 'efficiency' of discussions. The group was most active during the period following its creation in 2006, and is seen to have played a major role in highlighting to the Council the difficult relations between the national experts and the Commission. It increased the visibility of national experts and provided a platform for their complaints regarding the Commission's project management. Although the group's relevance decreased following the testing failures of 2008, when focus on national level preparations was diverted by the major technical problems affecting the central system, the

[76] As acknowledged by the Commission in a report of 2010: "….these different fora have contributed significantly to the elaboration of the present political and operational roadmap for the development of SIS II…". See Commission staff working document, Report on the global schedule and budget for the entry into operation of the second generation Schengen Information System (SIS II), SEC(2010) 1138 final, Brussels, 21.09.2010.

group is currently in the process of being revived as attention re-focuses on the preparations of national level systems.

The **Friends of SIS II** was created by the Council in February 2008 following the failure of the OST tests and in response to member states' doubts regarding the continuation of the SIS II project. Despite the group's title, the original initiative came from those member states most dubious about the project's future. However, these initial 'friends' or rather, SIS II sceptics, were soon joined by member states with an interest in keeping the project on course, and keen to ensure their views were represented in the group's discussions.

The group was set up at ministerial level, but in practice meetings have only been held at Sherpa level, between high-ranking officials and civil servants. It is chaired by the Council Presidency and the Commission participates, with national experts in attendance. The group's formal role as established in the Council conclusions of February 2008 was to support preparations for SIS II at national level, in cooperation with the SIS II Task Force. However, in practice the group has exceeded its mandate and has been influential in directing the decision-making process and in steering discussions on the central system. It emerged during interviews that the group fell out of favour after having been perceived to have made a number of misjudged decisions. Currently it is the least relevant of the groups working in SIS II, its role having waned since 2009 and replaced by a more recent formation, the Global Programme Management Board (GPMB).

The **GPMB** was established by the Commission in early 2009 in the midst of the ongoing crisis surrounding the technical problems of the central system. The aim was to diffuse the growing dissatisfaction among the member states with the SIS II project by granting them greater participation in its management and coordination. It was endorsed by the June 2009 Council which invited the Commission:

> to table and immediately implement an enhanced IT management structure and approach for the SIS II project…which ensures utmost transparency, insight and increased participation of the member states…[and] to this end further integrate the GPMB into the whole management structure.[77]

The GPMB has quickly become the most active and relevant group in steering the progress of the SIS II project, and in June 2010 its status was formalised with the adoption of the amended legal instruments governing migration to SIS II.[78] The group meets weekly and is chaired alternately by the Commission and the Presidency of the Council. In order to "ensure efficiency as well as cost effectiveness" membership is restricted to a maximum of eight national experts,[79] though participation is currently lower than this threshold. The low participation of this group partly reflects the degree of interest among member states as well as resource constraints. However, it also mirrors the highly politicised nature of membership in the GPMB (as well as the SIS II Task Force and the Friends of SIS II). For instance, the national experts of Austria, Germany and France initially participated in the group but were withdrawn when broad support could not be mobilized within the GPMB for the SIS 1+RE proposal.

[77] Conclusions of the JHA Council of 4-5 June 2009.

[78] Council Regulation 541/2010 amending Regulation (EC) No 1104/2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) OJ L 155/19, 22.6.2010; Council Regulation 542/2010 amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) OJ L 155/23, 22.6.2010.

[79] See Recital 4 and Article 17 (a) of Regulation 541/2010.

4.2 The role of expertise and knowledge in the legitimisation of power over SIS II

Analysis of the role played by EU level advisory bodies and working groups on SIS II yields several observations.

First, groups serve as a means for actors to gain influence over the SIS II project, allowing struggles and tensions to play out, and for common strategies to be forged between different actors. Certain national delegations and experts have attempted to use informal groupings to steer the direction of the project in accordance with their aims, withdrawing their experts if the group proved unable to meet their objectives. The potentially divisive role played by informal bodies is further exacerbated in view of their restricted membership. These groups often convene ahead of formal committee meetings involving all member states within the Council framework or the Commission's comitology structure. For instance, the Sherpa level of the Friends of SIS II group has traditionally met just before the high level preparatory body of the Council, the Article 36 Committee (CATS), and often functioned as a preparatory meeting for the decisions to be taken in this committee. It has emerged during the course of interviews that this timing allows the outcome of discussions in more formalised bodies to be 'pre-cooked' by experts in the informal or restricted groups. When experts of the restricted groups speak in formalised settings, it is often presumed that they are speaking on behalf of their board or task force. There are here strong echoes of the police-led networks which steered the construction of Schengen, facilitating information exchange and creating solidarities and divergences between nationalities and professions. Here again, through the groups, the field of governance on SIS II is marked by competition to collect information and exclude other actors.

Second, despite the range of bodies, each with a different mandate, there is a small, core group of experts who are present in almost all of the various working structures. There is little transparency surrounding this group, with reasons of security invoked for keeping the identity of these experts confidential. Yet these individuals – for the most part technology specialists from national police boards and ministries of interior – are invested with a considerable degree of power and responsibility. In an arena of fragmented decision-making, with little coordination between the respective working groups, they are among the few who are party to nearly all discussions at EU level on SIS II and are in a position to give a significant steer to the project within the GPMB, of which they are all members.

These actors draw authority from their position as technical experts, which confers legitimacy on their input to the project (Liberatore, 2007).[80] Their intervention is supposed to be 'de-politicised', ostensibly reduced to technical matters, although in practice the issues dealt with inside the groups extend beyond technical aspects.[81] It was also emphasised that members of the GPMB act in "a personal capacity" and do not represent any national or organisational interests. However, this neutrality could be questioned given that the same 'neutral' experts in the GPMB are required to change hats and attend comitology and council working parties where they represent their national ministries and report to their national police boards. It is no coincidence that, following the re-run of the second milestone test in 2010, the three experts who deemed the test failed were from Austria, France and Germany.

[80] As noted by Liberatore's assessment of the role of expertise in EU security policy: "Knowledge is a key asset in defining these authoritative actors….pluralism is limited to those actors who have the resources, including knowledge – that allow for inclusion in policy-making at EU level" (2007, p.109).

[81] The tendency to de-politicise the use of security technology through its framing as a technical rather than a legal or political concept has been identified as an important feature of securitisation (see Balzacq, 2008).

Third, with a central role accorded to expert knowledge, plural debate is limited. This, added to the semi-confidential character of proceedings surrounding certain groups raises questions regarding accountability and transparency. Actors with an important stake in the decision-making process on SIS II such as the European Parliament and the EDPS are excluded from participating in the groups and are only informed of the issues concerning the progress of the project on an informal, ad hoc basis. The problems of this lack of transparency were highlighted during a 2009 European Parliament debate on the state of play of SIS II, when MEPs complained that they had not been informed about the serious technical difficulties in the development of the new system, stating that they had had to learn about the problems through media reports.[82] Despite the reporting procedures put in place to inform the outcome of group discussions, these cannot entirely overcome criticisms of secrecy and in-transparency, as reports themselves are to some extent politicised. For instance, there have been tensions over the contents of reports from the SIS II Task Force to the high level CATS committee concerning the portrayal of the general progress of the project and member states' preparations.

5. Decision-making on SIS II: What result for accountability, proportionality and fundamental rights?

This section examines the main deficits stemming from the fragmented, inter-governmental, expert driven and emergency led policy-making approach that has characterised SIS II. There are three major issues of concern stemming from the analysis carried out in sections 2, 3 and 4 above: first, accountability and transparency; second, proportionality and efficacy of the final system; and third, the impact on the fundamental rights of third country nationals implicated by the SIS II.

5.1 Accountability, transparency and rule of law

A major criticism highlighted during the development of SIS II has been the lack of transparency and democratic accountability that characterised negotiations on the re-design of the system (Hobbing, 2005; Hayes, 2005). SIS II has been developed through numerous ad hoc amendments of the old rules contained in the 1990 Schengen Convention, rather than one clear, overarching legal document. This complexity is at least partly necessitated by the system's dual legal basis which required two legal instruments (a regulation and a decision) to regulate one system. However, it is also due to the delay in adopting a clear legal basis and the piecemeal approach taken by the Council with regard to negotiations on the functions and scope of SIS II. In 2003 the European Parliament criticised the so-called "salami tactics" approach of the Council with regard to decision-making on the SIS and SIS II in the lead-up to the adoption of the legal basis, arguing that parallel negotiations on different aspects of the SIS II pursued in different fora each with a different legal status would prevent a grasp of the full implications of the decisions taken. The rapporteur, Carlos Coelho, argued that:

> This approach is first of all very opaque, difficult to follow even by experts and completely incomprehensible for normal people. It is secondly not very democratic since formal legislative proposals only see the light of day after years of discussion in various Council working groups and only when a consensus among Member States is reached."[83]

Thus when the proposals for a regulation and decision on SIS II were finally presented in 2005, there was to some degree a sense of inevitability in the final outcome, with limited room for a public debate on the added value, necessity, scope and features of the new system. The inter-governmental origin of the Convention and the uncertainty surrounding the legal basis of SIS

[82] European Parliament CRE 11/03/2009, Debate on the State of Play of SIS II.

[83] Report with a proposal for a European Parliament recommendation to the Council on the second-generation Schengen information system (SIS II) of 7th November 2003, 2003/2180(INI).

enabled the development of SIS II to be obscured in a succession of non-binding documents produced by the Commission, Council and Presidency. Despite the application of the co-decision procedure, which meant that the European Parliament had an opportunity to influence the final text of the regulation and decision, the political urgency surrounding the adoption of the legislation meant that the Parliament agreed to a secret trialogue procedure, preventing a more open democratic debate, and a fast track adoption of the SIS II package at first reading. Similarly, the EDPS was granted an extremely tight calendar to examine the proposals on SIS II. The subsequent opinion delivered by the EDPS was the fastest to be prepared and submitted in the history of that body. It has been suggested that this may not have allowed for the degree of thoroughness required for monitoring such important legislative proposals.

As a result, the decisions on the new functionalities of SIS II and the marked shift in the purpose of SIS brought about by these changes have not been subject to the scrutiny and democratic oversight required by the rule of law principles substantiating the EU legal system. Furthermore, a lack of transparency and accountability remains in decision-making procedures surrounding the technical and political development of SIS II, to the extent that who is really deciding on the direction of SIS II is obscured. The presence of a complex network of committees, groups, boards and task forces, some without a formal mandate and several with restricted participation, enable a small group of national experts to play a strong role in steering the direction of the entire project. In parallel, fundamental decisions concerning the future of SIS II have increasingly been taken at the level of the Council, through Council Conclusions which are non-legal, political instruments characterised by a profound democratic deficit.

Finally, the difficult progress of the SIS II project, reinforced by interventions from member states, has undermined the Commission's perceived capability to develop large-scale EU IT systems. One perhaps unintended consequence is that this role will, in future, be transferred to the new (proposed) IT agency which is currently planned to assume responsibility for the management of SIS II and VIS and eventually other large-scale IT systems in the AFSJ.[84] It is currently not excluded that, beyond operational management, the IT agency may in the future be responsible for the *development* of large scale IT systems, a task which currently lies exclusively with the Commission.[85] The consequences of delegating such an important and sensitive task to an EU agency must be given serious reflection, particularly in view of the wider concerns raised regarding the transfer of powers to EU agencies and implications for accountability and transparency (see for example, Curtin, 2007).

5.2 Proportionate and efficient policy-making

Any security instrument adopted at EU level should be first subject to a test of proportionality. This principle is grounded upon two assumptions: first, that the EU acts only when it is required or it is necessary to do so in order to achieve a certain end, with the action entailing a balanced relationship between means and ends; and second, that the measures adopted are the least restrictive to freedom. The tendency for EU security policy strategies to by-pass these considerations has been noted by commentators (Guild and Carrera, 2011) and by the EDPS itself, which has underlined that: "a systematic approach in this area should be preferred to

[84] Commission proposal (amended) for a regulation on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2010)93 final, 19.03.2010.

[85] See Article 1 of the proposed regulation which states that "A European Agency for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS), EURODAC and for developing and managing other large-scale information technology ("IT") systems… is hereby established."

incident-driven policy-making, especially when incidents lead to the creation of new systems of data storage, collection and exchange without a proper assessment of existing alternatives."[86]

Assessing the proportionality of an initiative requires careful analysis of the evidence and a thorough assessment of a given measure's added value and effects. However, as we have seen, decisions on the technical feasibility of SIS II and its extended functions preceded any discussion at political level on the necessity or desirability of the new system. No impact assessment on the need for SIS II and the implications of its new functions has been conducted by the Commission or the Council, either before the start of the project's development or when the Commission presented its proposals in 2005.[87] A definitive assessment of the proposals' compliance with the principle of proportionality would perhaps have been difficult to establish regardless, given the concept of 'latent development' built into the SIS II architecture. As noted in the 2004 opinion of the Joint Supervisory Authority on SIS II:

> 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.[88]

Concerning the effectiveness and added-value of the SIS II, it is difficult to make such an assessment when the system is still far from operational. Nevertheless, the central question must be posed as to whether the benefits of the new system will justify the considerable financial resources invested in this project, both from the EU budget and from member states national purses. The costs for developing the central system are estimated at over €95 million. A further €35 million has been budgeted for the finalisation of the project, with over a third of this amount dedicated to hardware upgrades.[89] This represents an almost 500% increase on the original budgetary estimation for the project provided by the Commission in 2001.[90] These figures concern EU level payments on the central system. Expenditure on national systems has been estimated at approximately €20 million.[91] Further payments have been made available from the EU budget through the European Borders Fund, [92] in order to assist those smaller member states struggling to shoulder the mounting costs of the SIS II project.[93]

---

[86] Opinion of the European Data Protection Supervisor on the Commission Communication "The EU Counter-Terrorism Policy: main achievements and future challenges" OJ C 56/2, 22.2.2011.

[87] The likely explanation, as concluded in the House of Lords Report on the SIS II of 2006, was due to the intense political pressures to propose and adopt a legal basis as soon as possible to allow for the link up by the new member states. See House of Lords (2007), *Schengen Information System II (SIS II): Report with Evidence, 9th Report of Session 2006-2007*, European Union Committee, Stationery Office, London, p.15.

[88] Joint Supervisory Authority Opinion on the development of the SIS II, 19.05.2004.

[89] Commission staff working document, Report on the global schedule and budget for the entry into operation of the second generation Schengen Information System (SIS II) SEC(2010) 1138 final, 21.09.2010, Brussels.

[90] The original estimate of EU expenditure on SIS II was €23 million. See Commission Communication on Development of the Schengen Information System II, COM(2001) 720 final, 18.12.2001, p.20-21.

[91] Based on Dutch figures provided by the Dutch Minister of Internal Affairs (in Besters and Brom, 2010).

[92] Decision no. 574/2007/EC of the European Parliament and the Council of 23 May 2007 establishing the External Borders Fund for the period 2007-2013 as part of the general programme "Solidarity and management of migration flows", OJ L 144/22, 6.6.2007.

[93] It should further be taken into account that recourse to the SIS 1+RE solution would entail a considerable loss of resources invested in the SIS II project as well as additional expenditures.

That this substantial budgetary increase has so far delivered a system whose technical feasibility is still profoundly in question and future realisation uncertain has not gone unnoticed by the European Parliament. In a report of 2010, Rapporteur Carlos Coelho stated, "so as not to continue to throw good money after bad, particular rigour is called for in using appropriations for a system which has so far failed to reach the required standard."[94] Upon his recommendation, the Parliament froze funds allocated to the migration to SIS II at the end of 2010, only partially releasing them in early 2011.

The Commission has made a partial acknowledgment of the criticisms regarding the lack of proper consideration of the proportionality principle in a Communication adopted in July 2010.[95] The document intends to respond to concerns regarding the expansion of police and customs databases in the EU, by providing an overview of EU level measures regulating the management of personal information and proposing a set of principles, including "necessity" and "fundamental rights" intended to guide the future development and evaluation of any new measures. As the Commission recognises:

> Adopting such a principled approach to policy development and evaluation is expected to enhance the coherence and effectiveness of current and future instruments in a manner that fully respects citizens' fundamental rights.[96]

While such expressions are welcome, it is lamentable that these considerations are only now integrated into the EU's strategy on police cooperation and information management.

5.3 Fundamental rights

There are two aspects to consider regarding the repercussions of SIS II for fundamental rights, and more particularly data protection and privacy. First, it must be examined whether adequate efforts have been made to overcome the data protection gaps of the current SIS I. The second step is to examine the fundamental rights implications of the new functionalities built into the second generation of the system.

5.3.1 Addressing data protection gaps of the current SIS I?

The data protection deficiencies of the current SIS, as described in section 1.3 above, can be divided into the two following weaknesses:

1) Problems of data quality, caused by diverging practices of national authorities in reporting third country nationals.

2) Problems of access to judicial remedies, with legal and practical obstacles hindering individuals from contesting a wrongful listing in the SIS.

To what extent will SIS II overcome these gaps? Regarding data quality, the legal basis for the Regulation 1987/2006 on SIS II introduces a number of safeguards which may go some way to improve the accuracy and lawfulness of data contained in the system. The most important of these is the requirement that each decision to issue an alert must be taken on an "individual assessment" (Article 24.1) and the addition of a proportionality clause which stipulates that "before issuing an alert, member states shall determine whether the case is adequate, relevant

[94] Report on the proposal for a Council regulation amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System, A7-0127/2010, 29.04.2010.

[95] Commission Communication on an Overview of information management in the area of freedom, security and justice, COM(2010)385, Brussels, 20.7.2010.

[96] Commission Communication on an Overview of information management in the area of freedom, security and justice, COM(2010)385, Brussels, 20.7.2010, p. 28.

and important enough to warrant entry of the alert in SIS II" (Article 21).[97] The Regulation also includes stricter safeguards on data retention (Article 29) and the obligation to impose penalties for data inaccurately entered or unlawfully stored (Article 48).

Yet in spite of these improvements, the opportunity was nevertheless missed to provide for greater harmonisation of the grounds for reporting persons in the SIS. As seen above, an attempt by the European Commission to provide stricter grounds for entering a third country national in the draft legislation of the SIS II was rejected by member states. This means that the wide discrepancies in national reporting practices are likely to be replicated in SIS II. Given that SIS II will hold a great deal more (and more complex) data to be exchanged between an increased number of states, the scope for divergences, potential for inaccuracies and number of persons affected will be much larger.

Concerning access to remedies, the Regulation contains new data protection rules which are a welcome improvement on those provided by the CISA. Among these, the most important include the removal of the territorial restrictions on access to a judicial review and the inclusion of a new right to information in accordance with the EU's data protection directive (Article 42.1).[98] The provisions on audits and adequate resources for national supervisory authorities should also improve the quality and efficiency of supervision (Article 44), and the task of the EDPS to coordinate the national supervisory authorities could help ensure more rigorous oversight (Article 46).

On the other hand, Article 42. 1 on the right to information could have been strengthened further. This right is crucial as it is a pre-condition for securing an appeal against a wrongful listing in SIS. It is unfortunate therefore that the Regulation does not stipulate that individuals should be informed as soon as their details are entered in SIS II.[99] This may have a particular impact for third country nationals whose right of appeal may have expired by the time they are made aware of their listing, such as when they apply for a visa or arrive at the EU external border. The right to information is also subject to a number of exemptions, for instance, when the data has not been obtained directly from the third country national in question. This would apply in many of the cases in which a third country national to be refused entry is recorded in the SIS II (Brouwer, 2008: 530).

Furthermore, the possibility for an individual to access remedies against the wrongful entry of data in SIS II remains subject to the diversity of procedures under national law. For instance, it remains possible for national law to maintain the principle of indirect access to personal data (Article 41). Finally, there has been no explicit attempt to strengthen the legal position of third country nationals.[100] It remains the case that, while EU asylum and immigration instruments

[97] For a detailed discussion of the implications of the individual assessment requirement and proportionality clause, see Brouwer, 2008b.

[98] Article 42.1 refers to Articles 10 and 11 of Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31, 23.11.1995. The European Commission is currently planning to propose a new Data Protection Directive during the course of 2011 that should see a strengthening of the EU legal framework for data protection and privacy. See the Commission Communication on a comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 04.11.2010.

[99] Article 42.1 specifies that this information should be given in writing together with a copy or a reference of the decision giving rise to the alert, however there is no further rule regarding the timing of the notification.

[100] The wording of the right to remedies in Article 43 of Regulation 1987/2006 remains the same as its corresponding article in CISA.

generally refer to the right to legal remedies for third country nationals,[101] procedural rules are left to the scrutiny of the national administrator and access to a court is not guaranteed.

5.3.2 Risks implied by new functionalities

Several of the new capacities introduced in the SIS II raise a number of ethical concerns regarding their consistency with fundamental rights of the individual, in particular the use of biometric data, inter-linkage of alerts and potential inter-operability between EU databases.

The use of biometrics in EU border control and security instruments has been criticised by a wide range of organisations and experts due to the fallibility of this technology and its vulnerability to fraud.[102] Although initially the fingerprints and photographs stored in SIS II will only be used to confirm the identity of a person registered, Article 22 of the 2006 SIS II Regulation provides that "as soon as this becomes technically possible" fingerprints will be used as sole identifiers as well. This means that it would be possible to search the SIS II database using only fingerprints without the need for additional information. Under pressure from the European Parliament, the possibility for a biometric search function in the SIS II can only be activated subject to a Commission report on the availability and readiness of the available technology,[103] however the haste detected among member states to allow the biometric search function has led to the expectation that biometric searches will be enabled soon after SIS II becomes operational (Baldaccini, 2008).[104]

The potential use and misuse of biometric data not only risks undermining data quality further, it may also be at odds with fundamental rights restrictions on the use of personal data such as photographs and fingerprints. The taking of biometric information represents a violation of the right to private life enshrined in Article 8 ECHR unless the collection of data pursues a pressing social need and is legitimate and proportionate to that aim. Furthermore, EU data protection rules specify that personal data must only be collected for specific and legitimate purposes.[105] Limits on the collection and retention of biometric data were enforced in the European Court of Human Rights decision in *S & Marper v UK*, where the Court found the UK's arbitrary powers of retention of biometric data from persons suspected but not convicted of offences a disproportionate interference with the right to privacy and one that could not be considered necessary in a democratic society.[106]

Introducing linkages between alerts in the SIS II may be a logical tool for policing purposes but it poses questions regarding the effects on individuals, especially third country nationals. By allowing associations to be made between individuals stored for different purposes on the system, such as criminals with family members, or irregular migrants with traffickers, this

---

[101] See Brouwer, 2008b and 2007b. This assessment was supported by the Court of Justice in its ruling in the Panaytova case of 16 November 2004 where the CJEU made it clear that the general principles of effective remedies in relation to EU rights also apply in the field of immigration law procedures, Case C-327/02 *Panayotova* [2004] ECR I-11055.

[102] See for example the Opinion of the European Data Protection Supervisor on VIS, Brussels, 23.03.2005. See also the Opinion of the EDPS on SIS II, in which he cites the case of a US lawyer wrongly identified and detained as a terrorist because his fingerprints matched those found in the bombings on Madrid.

[103] This provision was inserted in Article 22 (c) of the SIS II Regulation and Decision at the behest of the European Parliament.

[104] See Council conclusions on the SIS, No. 10586/07 of 08.06.2007.

[105] Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31, 23.11.1995.

[106] *S & Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, ECtHR, Judgement of 4 December 2008. For further discussion of this case, see Guild, 2010.

function opens the door for increased breaches of the purpose principle and paves the way for further stigmatisation of certain categories of individuals, i.e. third country nationals seeking entry and residence in the EU. This is particularly true in light of the fact that this database is used both for immigration and criminal law purposes, meaning that individuals registered for immigration reasons may be at greater risk of becoming the targets of criminal law enforcement measures or secret surveillance. The possibility for 'criminal networks' or 'immigration networks' to be progressively registered is not excluded. Interlinking thus allows an 'intelligence' logic to creep into the use of the system, further deepening associations between crime and migration and increasing the chances of negatively impacting on innocent persons.

The singling out of migrants as a potential risk category in this way could stand in tension with EU principles of non-discrimination. The discriminatory potential of different data processing practices which monitor more strictly and systematically one group of individuals over another was highlighted by the Court of Justice in the case *Heinz Huber* v *Germany*.[107] In particular, the Advocate-General appointed to the case argued that differentiated data processing practice (in this case between nationals and non-national EU citizens) casts "an unpleasant shadow" over the groups subject to a stricter monitoring and that reasons of crime and threats to security cannot justify such discriminatory treatment.[108] The Huber judgement is central here as it underlines the discriminatory implications of databases which single out third country nationals, especially in view of the indirect effects of secondary uses of information originally stored for other purposes (González Fuster, De Hert, Ellyne and Gutwirth, 2010).

Dangers associated with the transformation of SIS II into an investigative tool are further compounded by the technical possibility for SIS II to become 'interoperable' with other large-scale EU databases. Interoperability, the possibility to share access and exchange data between IT systems – has been promoted in the name of crime prevention or counter-terrorism in EU policy discussions for some time, supported by the Commission in a Communication of 2005 on enhanced interoperability of databases.[109] Despite their very different legal characteristics, rationale, and the fact that the member states participating in the systems and authorities granted access differ, the potential future integration of EU databases such as SIS II, VIS and Eurodac has already been progressively built into their design (González Fuster, Gutwirth, and De Hert, 2009; Geyer, 2008).

The EDPS has issued strong warnings against the move towards interoperability, particularly concerning the risk of contravening the purpose principle.[110] Despite these cautions, the proposal for a new EU level IT agency to manage SIS II and VIS and eventually other large-scale EU IT systems risks a further shift in the direction of a technical inter-linkage between different EU databases.[111] The strategic importance of this management authority is reflected in the struggle between the governments of Estonia and France for hosting the agency's seat. The

[107] Case C-524/06 *Huber v Germany* [2008] ECR I-9705.

[108] Opinion of Advocate General Poiares Maduro in Case C-524/06 *Huber v Germany*, delivered on 3 April 2008.

[109] Commission Communication on improved effectiveness, enhanced inter-operability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, 24.11.2005, Brussels. For an analysis of this communication see De Hert and Gutwirth, 2006.

[110] Opinion of the European Data Protection Supervisor on the Commission Communication on an Area of Freedom, Security and Justice Serving the Citizen, 10.07.2009. It might be noted that the EDPS has, over time, softened its stance towards inter-operability, now underlining that it should be implemented on condition that is accompanied by relevant safeguards. See for instance, EDPS, *Annual Report 2009*, Luxembourg, Publications Office of the European Union, p.52.

[111] Commission proposal (amended) for a regulation on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2010)93 final, 19.03.2010.

dispute was finally resolved with a compromise agreement which will see the agency split between Tallinn and Strasbourg locating the administrative headquarters in Tallinn, but the operational management in Strasbourg. The EDPS has registered its concern with the Agency's powers and underscored the need to introduce a series of safeguards to the current legislative proposals.[112]

Conclusions and recommendations

This paper set out to examine the development of the Schengen Information System II, to identify the factors at the root of the project's delays and ethical deficiencies and to draw lessons for the future development of large-scale EU level (surveillance) databases.

The paper finds that the decision-making processes surrounding SIS II bear all the hallmarks of the 'pioneer' spirit of Schengen, of struggles between EU and intergovernmental competence, of a policy process driven by security 'threats' and shaped by the input of national police and technical experts. Yet the SIS II project – considerably over-budget and with no guarantee of completion – provides a strong critique of the Schengen 'laboratory' model of cooperation and should serve as a cautionary tale for EU policy-makers considering the development of future large-scale databases for the AFSJ. Instruments developed outside the proper EU policy-making procedures, even when eventually transplanted into the EU framework, retain the traits – and replicate the deficiencies – of inter-governmental decision-making in this domain.

Indeed, the paper finds that both the technical problems and fundamental rights weaknesses of SIS II are strongly linked to struggles between the EU and the intergovernmental methods of cooperation and the fragmented and piecemeal approach that characterised decision-making on SIS II from the outset. The legal uncertainty surrounding SIS II before the adoption of the legal basis in 2006 meant that the system was designed through a highly in-transparent process under the (former) third pillar. New features and functionalities of SIS II were elaborated by representatives of national police, interior ministries, and experts of security technology, with agreements made in non-binding Council conclusions. This process was given impetus by the events of 9/11, where the sense of emergency created by the 'new terrorist threat' was used to frame discussions on SIS II and forge agreement on a number of controversial new features such as the addition of biometrics and extended access to police authorities, such as Europol.

Even after endowing the European Commission with the competence to manage the SIS II project, and following the expansion of the co-decision procedure which further strengthened the legislative roles of the Commission and European Parliament, (certain) member states were not ready to relinquish control of a tool so central to security and migration management. Strategies to retain ownership of the project emerged, including the proliferation of expert groups, and the SIS1+RE proposal for an 'intergovernmental' alternative to SIS II. The latter in particular represents a direct political challenge to the Commission, one that, if adopted, would seriously undermine the professional capacity of this institution to develop and deliver an EU instrument governing internal security. In this vein, the SIS1+RE proposal may be interpreted as an attempt to 'clip the wings' of the Commission; part of an underlying strategy by certain member states to restrict the Commission's efforts to elaborate an integrated approach to EU information management in the field of security and surveillance. It appears that successive proposals for more and bigger databases at EU level which are steadily creating a complex

[112] The EDPS commented that: "The creation of an Agency for such large-scale databases must be based on legislation which is unambiguous about the competences and the scope of activities of the Agency. Such clarity would prevent any future misunderstanding about the conduct of the agency and avoid the risk of function creep. As currently drafted, the proposals do not meet those standards." See Opinion of the European Data Protection Supervisor on the proposal for a Regulation establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 7.12.2009.

supranational security architecture may sit uneasily with member state prerogatives to retain powers over internal security and channels of information (Geyer, 2008).

However, the cost of such institutional struggles is high in terms of legal uncertainty and insecurity, and it is the individual, particularly third country nationals, who ultimately pay the price. Paradoxically, the development of the most important database in the EU's AFSJ, a tool intended to deliver security, could serve to erode the freedoms and liberties of the individual. The new functionalities of SIS II pose profound ethical challenges in light of EU principles of non-discrimination, data protection and privacy. That decision-making on these new functionalities has taken place beyond the framework of judicial and democratic scrutiny threatens to undermine the political legitimacy of the AFSJ. According to the ECtHR, the legality of such surveillance measures hinges on whether they are judged "necessary in a democratic society". Yet justification of the democratic necessity of SIS II has still to be provided. With a series of new, large-scale EU databases, such as the VIS, the entry/exit system and the Passenger Name Record system currently in the pipeline, a full account by the Commission of the necessity and impact of these costly security technologies is urgently required. Without a close re-assessment of the EU's strategy on information exchange, SIS II may not be the last expensive experiment in EU surveillance technology to have serious consequences for fundamental rights.

In view of the evidence brought to light by this paper, the following policy recommendations can be drawn:

- SIS II has been shaped by the politics of emergency. Henceforward, steps should be taken to ensure that an ***evidence-based approach prevails over incident driven policy-making***. This implies a genuine assessment of whether new tools for information exchange will increase internal security in the EU, based on full consideration of the principles of necessity, efficiency, proportionality and fundamental rights. Advancing the EU strategy on information management should begin with an *independent* inventory of current policies, tools and institutional structures involved in data exchange in the field of security at EU level, building on the Commission's preliminary mapping exercise undertaken in 2010.[113] Such an inventory could feed into the forthcoming communication on the European Information Exchange Model scheduled for 2012 which should be used as an opportunity for a genuine re-assessment of the value and appropriateness of current instruments, and not an opportunity to propose new and unnecessary measures.[114]
- The SIS II has not yet proved to be proportionate, safe and reliable. ***No new database should be set up*** until SIS II is found to have met these criteria. Both DG Justice, Citizenship and Fundamental Rights of the European Commission and the Fundamental rights Agency (FRA) should be engaged to conduct a fundamental rights proof-reading of SIS II, taking into account the risks implied by its potential inter-operability with other large scale databases. This assessment should include a comparison of the impact of the current SIS on fundamental rights and the extent to which SIS II will replicate/overcome these deficiencies. Should the SIS II fail its second milestone test, neither the SIS 1+RE, nor any other alternative to SIS II should be developed until a

[113] Commission Communication on an Overview of information management in the area of freedom, security and justice, COM(2010)385, Brussels, 20.7.2010.

[114] The Stockholm Programme calls on the European Commission to: "assess the need for developing a European Information Exchange Model based on the evaluation of the current instruments… These assessments will determine whether these instruments function as originally intended and meet the goals of the Information Management Strategy". See Council of the European Union, The Stockholm Programme – An open and secure Europe serving and protecting the citizens, 17024/09, Brussels, 2 December, 2009.

thorough assessment has been made of the ethical, efficacy and financial implications and a clear allocation of responsibility for the development of the alternative system has been defined in advance. If the decision is taken to delegate to member states the development of an alternative scenario for a transitional period, it must justify how the financial and legal accountability of those member states will be ensured.

- An unrealistic timetable exerted artificial pressures on the decision-making process on SIS II. ***Overambitious political timetables should be avoided***, particularly in matters concerning the AFSJ and in areas as sensitive as security policy. They can weaken budgetary oversight, allowing financial expenditures to escalate. Moreover, by sidelining proper democratic and judicial scrutiny of new security technology measures, they risk undermining fundamental rights and the rule of law, and lead to more insecurity for the individual. [115]
- Decisions on SIS II have largely been taken behind closed doors, in expert working groups and (until recently) with limited involvement of the European Parliament. The ***democratic accountability*** of policy-making relating to the development of large-scale EU databases must be ensured by ***allowing the European Parliament to play its full role*** in the policy process. Parliament should be fully informed of discussions and developments and given sufficient time to scrutinise proposals for future EU large-scale IT systems. The use of informal trialogue procedures should not be used to fast-track legislative proposals. Where trialogue procedures undermine transparency and remove the opportunity for open and plural debate, they are counterproductive. Likewise, the Parliament does not need to rely on the speed by which it passes legislation to prove itself as a responsible co-legislator (despite pressures to the contrary). Efficiency is measured not through speed but the extent to which the Parliament exercises democratic scrutiny of the legislative process, in fulfillment of its role as guardian of liberties and democracy in the EU. It is worth recalling that in the case of SIS II, it was the European Parliament that brought forward questions of fundamental rights and budgetary oversight. Given the central role of the Parliament in holding policymakers accountable to citizens (and taxpayers), the LIBE committee could take steps to strengthen its scrutiny of large-scale IT systems. This may require upgrading the current informal Privacy Platform into a formal Working Group or establishing a new working group looking more specifically at issues related to the EU information management strategy, including but not limited to privacy aspects. This working group would contribute to discussions surrounding the European Information Exchange Model and the desirable way forward for large scale EU IT systems by considering the real necessity of these instruments for internal security, as well as their impact on fundamental rights and budgets.
- Expertise has been privileged in decision-making on SIS II, to the exclusion of other voices. In developing future large scale IT systems, the ***role of experts should be re-assessed and counter-balanced*** by allowing a plurality of actors and perspectives to provide input to the policy process. A close and formalised partnership should be ensured with the FRA, the EDPS and the Article 29 Data Protection Working Party in the phases preceding the formal adoption of proposals and when monitoring their implementation to assess the ethical impacts, added value and practical effectiveness of large-scale EU IT systems. This should be complemented with open consultation mechanisms with other key stakeholders, such as practitioners and civil society organisations.

[115] See also the policy recommendations stemming from F. Geyer's analysis of databases in the AFSJ (2008).

- The SIS II experience has led directly to the decision to create an ***agency for the operational management of large-scale IT systems*** in the AFSJ. Appropriate safeguards must be included in the legislation establishing the agency in order to avoid the risk of function creep and prevent infringements of the principle of purpose limitation. Legislation must be clear about the competences and clearly define and limit the scope of activities of the agency. The agency should operate in a transparent manner subject to democratic oversight by the European Parliament. The Parliament should therefore participate in the selection procedure for the agency's Executive Director and receive regular reports from the agency's management board.
- The ethical dimension has not been part of the policy process of SIS II. Respect for ***fundamental rights and data protection*** must move to the centre of future policy strategies for developing large-scale IT systems in the AFSJ. The impact of new databases or any evolution in the use of current security technology on the individual should be carefully and independently assessed and properly considered by the relevant Commission services before any new initiative is presented. This should be complemented with the application by DG Justice, Citizenship and Fundamental Rights, of the Commission's new methodology for evaluating EU policy compliance with the Charter of Fundamental Rights.[116] Further, "data protection by design", allowing for automated solutions to data protection requirements such as automatic deletion of data at the end of the permitted period, should be made an obligatory feature in the implementation of new and existing databases. Individuals must be adequately protected against the consequences of data inaccuracies or of negligent data exchange and must be properly informed of their rights.[117]

[116] See Commission Communication on a Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM(2010) 573, Brussels, 19.10.2010.

[117] See also the final policy recommendations of the Challenge Project (Changing landscape of European Liberty and Security) under the section 'Data Protection.' (Bigo, Carrera and Guild, 2009).

References

Baldaccini, A. (2008) "Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases", *European Journal of Migration and Law*, Vol. 10, pp. 31 – 49.

Balzacq, T. (2008), "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies," *Journal of Common Market Studies*, Vol. 46, No.1, pp. 75-100.

Bertozzi, S. (2008a), *Schengen: achievements and challenges in managing an area encompassing 3.6 million km2* CEPS Working Document No. 284, February 2008.

Besters, M. and F. Brom (2010), "'Greedy' Information Technology: The Digitalisation of the European Migration Policy", *European Journal of Migration and Law*, Vol.12, pp.455-470.

Besters, M. (2010), "De schaduwzijden van het Schengen Informatie Systeem" in G. Munnichs, M. Schuijff & M. Besters (eds.) *Databases: Over ICT-beloftes, informatiehonger en digitale autonomie*, Rathenau Instituut, The Hague.

Bigo, D. (1996), *Polices en Réseaux: l'Expérience Européenne*, Presse de Sciences Po, Paris.

Bigo, D. and S. Carrera (2004), *From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU*, CEPS Commentary.

Bigo, D., S. Carrera and E. Guild (2009), *The CHALLENGE Project: Final Policy Recommendations on the Changing Landscape of European Liberty and Security*, CHALLENGE Research Paper No. 6, September 2009.

Bigo, D. and Jeandesboz, J. (2010), *The EU and the European Security Industry: Questioning the 'Public-Private Dialogue,'* INEX Policy Brief No. 5, February 2010.

Broeders, D. (2007), "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants", *International Sociology*, Vol. 22, pp.71-92.

Brouwer, E. (2002), "Immigration, Asylum and Terrorism: A Changing Dynamic Legal and Practical Developments in the EU in Response to the Terrorist Attacks of 11.09", *European Journal of Migration and Law*, Vol.4, pp. 399 – 424.

Brouwer, E., P. Catz & E. Guild, (eds) (2003) *Immigration, Asylum and Terrorism: A Changing Dynamic in European Law*, Nijmegen, Recht & Samenleving.

Brouwer, E. (2007a), "The Use of Biometrics in EU Databases and Identity Documents: Keeping Track of Foreigner's Movements and Rights" in J. Lodge (ed.), *Are You Who You Say You Are? The EU and Biometric Borders*. Nijmegen, Wolf Legal Publisher, pp. 45-66.

Brouwer, E. (2007b), "Effective Remedies in EU Migration Law" in A. Baldaccini, E. Guild and H. Toner (eds.) *Whose freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, Oxford.

Brouwer, E. (2008), *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System* Leiden, Martinus Nijhoff Publishers.

Brouwer, E. (2008b), *The Other Side of the Moon: The Schengen Information System and Human Rights – A Task for National Courts*, CEPS Working Document, No.288, April 2008.

Bunyan, T. (2002) *The War on Freedom and Democracy: an Analysis of the Effects on Civil Liberties and Democratic Culture in the EU*, Statewatch, (available at: http://www.statewatch.org/news/2002/sep/04freedom.htm).

Busch, H. (2006), *Statewatch Analysis: The Dream of Total Data Collection – Status Quo and Future Plans for EU Information Systems*, Statewatch Bulletin, London.

Carrera, S. (2005), "What Does Free Movement Mean in Theory and Practice in an Enlarged EU?" *European Law Journal*, Vol.11, No.6, pp. 699-721.

Cholewinski, R. (2007), "The Criminalisation of Migration in EU Law and Policy," in A. Baldaccini, E. Guild and H. Toner (eds.) *Whose freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, Oxford.

Craig, P. and G. De Burca (2008), *EU Law: Text, Cases and Materials*, Oxford University Press, Oxford.

Curtin, D. (2007), "Holding (Quasi-)Autonomous EU Administrative Actors to Public Account," *European Law Journal*, Vol. 13, No. 4, pp.523-541.

De Hert, P. and S. Gutwirth (2006), "Interoperability of Police Databases within the EU: An Accountable Political Choice?" *International Review of Law, Computers and Technology*, Vol. 20, No. 1, pp.21-35.

De Zwaan, J.W. (1998), "Schengen and its Incorporation into the New Treaty: the Negotiating Process", in M. Den Boer (ed.), *Schengen's Final Days? The Incorporation of Schengen into the New TEU, External Borders and Information Systems*, European Institute of Public Administration, Maastricht.

Den Boer, M. (2002), "To What Extent Can There Be Flexibility in the Application of Schengen in the New Member States?" in M. Anderson and J. Apap (eds.), *Police and Judicial Cooperation and the New European Borders*, The Hague, Kluwer.

Edwards, G. and E. Philippart (1999), "The Provisions on Closer Cooperation in the Treaty of Amsterdam: the Politics of Flexibility in the European Union", *Journal of Common Market Studies*, Vol.37, No. 1, pp.87-108.

Faure-Atger, A (2008), *The Abolition of Internal Border Checks in an Enlarged Schengen Area*, CHALLENGE Research Paper No.8, Centre for European Policy Studies.

Geyer, F. (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS Challenge Research Paper No. 9, May 2008.

Garside, A. (2006), *The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU?* Sussex Centre for Migration Research, Sussex Migration Working Paper No. 30.

González Fuster, G., S. Gutwirth, and P. De Hert, (2010) *Analysis of the value dimensions of European law relevant to current and anticipated challenges of the internal/external security continuum*, Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology & Society (LSTS), INEX Working Paper.

González Fuster, G., P. De Hert, E. Ellyne and S. Gutwirth (2010), *Huber, Marper and Others: Throwing New Light on the Shadows of Suspicion*, INEX Policy Brief, No.8, June 2010.

Groenendijk, K. (2004), "Reinstatement of Controls at the Internal Borders of Europe: Why and Against Whom?", *European Journal of Migration and Law*, Vol.10, No. 2, pp. 150-170.

Guild, E. (2001), *Moving the Borders of Europe*, Inaugural lecture, University of Nijmegen.

Guild, E. and D. Bigo (2002), "The Legal Mechanisms – Collectively Specifying the Individual: The Schengen Border System and Enlargement" in M. Anderson and J. Apap (eds.), *Police and Judicial Cooperation and the New European Borders*, The Hague, Kluwer.

Guild, E., S. Carrera and T. Balzacq (2008), *The Changing Dynamics of Security in an Enlarged European Union* CHALLENGE Research Paper No. 12, Centre for European Policy Studies.

Guild, E. (2010), *Global Data Transfers: the Human Rights Implications*, INEX Policy Brief, No.9, May 2010.

Guild, E. and Carrera, S. (2011), *Towards an Internal (In)security Strategy for the EU?* CEPS Liberty and Security in Europe series, January 2011.

Hayes, B. (2004), *From the Schengen Information System to SIS II and the Visa Information System (VIS): the Proposals Explained*, Statewatch Analysis, February 2004.

Hayes, B. (2005), *SIS II: Fait Accompli? Construction of the EU's Big Brother Database Underway*, Statewatch Analysis, May 2005.

Hayes, B (2008), *Schengen Information System Article 99 Report: 33,541 people registered in SIS for surveillance and checks*, Statewatch Analysis, February 2008.

Hobbing, P. (2006), *An assessment of the proposals of regulation and decision which define the purpose, functionality and responsibilities of the future SIS II*, Briefing Paper for Directorate C of the European Parliament, IP/C/LIBE/OF/2005-168, 15 February 2006.

House of Lords (2007), *Schengen Information System II (SIS II): Report with Evidence, 9th Report of Session 2006-2007*, European Union Committee, Stationery Office, London.

Jeandesboz, J. (2010), "Logiques et Pratiques de Contrôle et de Surveillance des frontières de l'Union européenne" in A. Scherrer, E. Guittet and D. Bigo (eds.), *Mobilités sous Surveillance: Perspectives Croisées UE-Canada*, Paris, Cultures et Conflits.

Karanja, S. (2008), *Transparency and Proportionality in the Schengen Information System and Border Control Cooperation*, Leiden, Martinus Nijhoff.

Liberatore, A. (2007), "Balancing security and democracy, and the role of expertise: biometric politics in the European Union", *European Journal on Criminal Policy and Research*, Vol. 13, pp.109-137.

Mitsilegas, V. (2007), "Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance", in A. Baldaccini, E. Guild and H. Toner (eds.) *Whose freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, Oxford.

Monar, J. (2001), "The Dynamics of Justice and Home Affairs: Laboratories, Driving Factors and Costs", *Journal of Common Market Studies*, Vol. 39, No. 4, pp. 747-764.

Monar, J. (2002), "The Problems of Balance in EU Justice and Home Affairs and the Impact of 11 September" in M. Anderson and J. Apap (eds.), *Police and Judicial Cooperation and the New European Borders*, The Hague, Kluwer.

Pastore, F. (2002), "The Asymmetrical Fortress: the Problem of Relations between Internal and External Security Policies in the European Union" in M. Anderson and J. Apap (eds.), *Police and Judicial Cooperation and the New European Borders*, The Hague, Kluwer.

Peers, S. (2008), "Key Legislative Developments on Migration in the European Union: SIS II", *European Journal of Migration and Law*, Vol.10, pp.77-104.

Stubb, A. (1996), "A Categorisation of Differentiated Integration", *Journal of Common Market Studies*, Vol. 34, No. 2, pp.283-295.

Weiler, J (1999), "Epilogue: 'Comitology' as Revolution – Infranationalism, Constitutionalism and Democracy", in C. Joerges and E. Vos (eds.), *EU Committees: Social Regulation, Law and Politics*, Oxford, Hart.

Zaiotti, R (2011), *Cultures of Border Control: Schengen and the Evolution of European Frontiers*, Chicago, University of Chicago Press.

Annex 1. Table of Commission Committee, working and advisory groups and preparatory and informal groups of the Council related to the SIS II project

Title of Group	Status	Participating member states	Role of Commission	Mandate and tasks	Reporting	Main period of activity
The Global Programme Management Board (GPMB)	Initially informal, established by Council conclusions 26-27 February 2009. Formalised in 2010 (Regulations 541&542/2010)	Experts are nominated in their role as experts not as representatives of member states or associated countries. Experts originating from Sweden, Netherlands, Portugal, Norway and Hungary have been nominated, plus an expert from the member state holding the Presidency of the Council. Private contractors and any other relevant expert can be invited to attend	Alternate chairmanship with Council Presidency	Advisory board for assistance to the central SIS II project and shall facilitate consistency between central and national SIS II projects.	Formal reporting procedure to SISVIS committee and relevant Council preparatory bodies (as appropriate)	February 2009 - ongoing
The Friends of SIS II (FoSIS)	Informal. Established by Council conclusions of 28 February 2008	Initial composition: Czech Republic, Germany, Spain, France, Italy, the Netherlands, Austria, Poland, Portugal, Slovenia, Finland, Sweden, Norway and the UK (No information available on current composition)	One Commission representative participates	To follow and support the SIS II development in the Member States. Meetings at "Sherpa" level aim to provide a bridge between expert and ministerial levels.	Reports to CATS (informal reporting procedure)	February 2008 - 2009
The SIS II Task Force (SIS II TF)	Informal. Established by Council	Initial composition: Austria, Czech Republic, France, Germany, Italy, Norway, Poland, Portugal, Sweden,	None	To assist in the management and coordination of the SIS II project, including the state of preparedness of Member States.	Reports to CATS (informal reporting	October 2006 – 2008

	conclusions of 5 October 2006	Slovenia, the Netherlands and the UK (No information available on current composition)		Group makes recommendations to CATS committee.	procedure)	
SISVIS Committee (sits in three formations)	Formal committee (Regulation 1987/2006) & Decision 2007/533/JHA	All member states. Schengen associated countries may attend. Europol and Eurojust may attend. Private contractors also invited to attend	Chair	To assist the Commission when taking certain specific measures in the context of SIS II development and operations under the comitology procedure.	summary report is sent to the European Parliament	2007 - ongoing
SISVIS Committee (SIS II TECHNICAL Formation)	Formal committee (Regulation 1987/2006) & Decision 2007/533/JHA	All Member States. Schengen associated countries may attend.	Chair	To assist the Commission when taking certain specific measures in the context of SIS II development and operations under the comitology procedure.	Is a formation of the SISVIS committee	2007 - ongoing
SISVIS Committee (SIS SIRENE Formation)	Formal committee (Regulation 1987/2006) & Decision 2007/533/JHA	All Member States. Schengen associated countries may attend.	Chair	To assist the Commission when taking certain specific measures in the context of SIS II development and operations under the comitology procedure.	Is a formation of the SISVIS committee	2007 - ongoing
Change Management Board (CMB)	Established by SISVIS Committee	Member states' experts (including representatives of the current and next presidency) Main development contractor. Ad hoc technical experts.	Chair	Advisory working group of the SISVIS Committee that examines issues related to corrections and requests for changes in the technical specifications and implementation of SIS II.	Submits regular reports to the SIS VIS committee	2008
Test Advisory Group (TAG)	Established by SISVIS Committee	Member states' experts (which ones?) (including representatives of the current and next presidency) Main development contractor. Ad	Chair	Advisory working group of the SIS VIS Committee that examines issues related to certain SIS II tests. Reports help prepare SISVIS committee to prepare	Submits regular reports to the SIS VIS committee	2008

		hoc technical experts.		decisions related to tests and their validation.		
National Project Managers meeting (NPM)	Informal	All member states. Schengen associated countries may attend.	Chair	Meeting of national project managers, discusses the development of the SIS II project and if necessary prepares items for the SISVIS committee.	Advises the Commission on an informal basis	2005 ongoing
Article 36 Committee (CATS)	Formal Council working group	All member states (plus associated Schengen countries in the CATS Mixed Committee) The Committee is made up of senior officials Europol and Eurojust are invited to attend	Commission representatives are invited to attend	Coordinates the competent working groups in the field of police and judicial cooperation. Also prepares the relevant work of the Permanent Representatives Committee.	Reports to COREPER	1999 - ongoing
Working Party on Schengen Matters (SIS-TECH formation)	Formal Council working group	All member states (plus associated Schengen countries in the CATS Mixed Committee) Europol and Eurojust are invited to attend	Commission representatives are invited to attend	Monitors the functioning of SIS and advises the CATS committee regarding operating and technical issues associated with the functioning of SIS.	Reports to CATS (and to SIS-SIRENE formation on financial matters)	1999-ongoing (with reforms)
Working Party on Schengen Matters (SIS-SIRENE formation)	Formal Council working group	All member states (plus associated Schengen countries in the CATS Mixed Committee) Europol and Eurojust are invited to attend	Commission representatives are invited to attend	Monitors and advises CATS committee regarding the practical, operational, economic and (to some extent) legal issues concerning the Schengen Information System (SIS) and the national office, Sirene, which is the single contact point for the exchange of supplementary information related to SIS data.	Reports to CATS	1999-ongoing (with reforms)