## Statewatch Analysis

# The SIS II proposals

### Introduction

At the end of May 2005, the Commission finally released legislative proposals to govern the next generation of the Schengen Information System (SIS), a massive database including data used by policing, border control, visa, criminal law and immigration authorities (and soon vehicle registration bodies) across Europe. These proposals would add more types of data to the Schengen Information System (particularly fingerprints and photographs) and would release data to more authorities—particularly the authorities responsible for expulsion and asylum. The following sets out the background to these proposals, followed by a detailed analysis and critique of key issues.

In many respects the proposals are highly unclear, particularly as regards the key issue of data protection rights and the grounds for inclusion of information on people to be banned from the Schengen area. In part persons could be banned from the Schengen area based on application of EC legislation that has not yet been proposed! There has been no impact assessment and many details of the proposals do not seem to have been fully thought through. Above all, the legislative process as regards these proposals is in many respects a sham, as the Council has already decided on the key functions of the next version of the SIS without any democratic consultation (or impact assessment) whatsoever and the Commission has already awarded the tender to set up SIS II, following a controversial tender process. In any event, the Commission has not seen fit to explain any of the complex text of its proposals.

Given this non-existent democratic scrutiny, dubious financial accountability, unjustified extensions of access to data and ambiguous provisions on data protection and the grounds for people to be banned from the entire Schengen area, these proposals represent another step in the construction of a European 'surveillance society'.

### Background

#### *The overall framework of the SIS*

The basic rules governing the Schengen Information System (SIS) are set out in Articles 92-119 of the Schengen Convention (OJ 2000 L 239). Further rules are set out in various decisions of the Schengen Executive Committee (also in OJ

2000 L 239), including the Decision establishing the Sirene manual (the manual governing subsequent exchanges of information following a 'hit' in the SIS (OJ 2003 L 38).

The SIS applies currently to thirteen Member States (all the 'old' Member States except the UK and Ireland), plus associated states Norway and Iceland. It will apply in part to the UK and Ireland (except as regards immigration data) in the near future, when the conditions for those states to apply SIS rules are met. It cannot apply to the new Member States which joined the EU in 2004 (or to Switzerland, which has signed a treaty to become another Schengen associate member) until the capacity of the system is expanded to accommodate more countries. This expansion is one reason for the creation of the second version of the SIS (SIS II); the more controversial reason is the plans to expand the SIS to include new categories of alert, new categories of data, linked alerts and wider access to SIS data.

With the entry into force of the Treaty of Amsterdam in May 1999, the Schengen acquis was integrated into the EU legal order. But since it proved impossible to agree on how to 'allocate' the provisions on the SIS between the first pillar (EC law, including visas, borders and immigration law) and the third pillar (EU law, concerning policing and criminal law), the SIS provisions were provisionally allocated to the third pillar. But any later measures building on the Schengen acquis have to be based on the correct 'legal base' – entailing use of the Community legal system and decision-making procedures for any amendments relating to the immigration data contained in the SIS.

Several EC and EU measures have been adopted concerning the SIS since 1999. In 2001, a parallel first pillar Regulation and third pillar decision were adopted, giving the Commission the responsibility of managing the development of the planned 'SIS II'. In 2004 and 2005, a parallel Regulation and Decision were adopted, providing *inter alia* for the inclusion of new categories of data and wider access to SIS data. Also, in 2004, a parallel Regulation and Decision were adopted to confer upon the Commission the power to amend the Sirene manual. The Commission has not yet exercised these powers, although it has embarked upon consultation with Member States as a precursor to using them. Finally, in June 2005, the Council and European Parliament (EP) adopted a regulation permitting vehicle registration authorities to search the SIS.

At the end of May 2005, the Commission finally made formal proposals to establish SIS II. These consist of:

a) a Regulation (to be adopted by qualified majority voting in the Council of national ministers and co-decision with the EP) which would govern the immigration law aspects of the SIS;
b) a third-pillar Decision (to be adopted by unanimous voting in the Council and consultation of the EP) which would govern the use of the SIS for policing and criminal law data; and
c) a Regulation (to be adopted by qualified majority voting in the Council and co-decision with the EP) which would govern the access to SIS data by vehicle registration authorities

But well before the Commission's formal proposals, the Council adopted successive conclusions in 2002, 2003 and 2004 on the functions that SIS II should have. The Council also adopted conclusions in 2004 on the financing and operational management of SIS II, although these conclusions leave some key questions open. Following these conclusions, the Commission completed the tendering process for SIS II (along with the parallel planned VIS: the Visa Information System) in autumn 2004. The Commission's application of the rules on tendering in this case was so controversial that a disappointed tenderer sued the Commission, which was criticised for its practices by the Court of First Instance, although the case was later withdrawn. But if this contract is cancelled or amended now, the EU is presumably financially liable to the contractor. So to a large extent, as pointed out above, the legislative proposals simply 'rubber-stamp' agreements on SIS II that have been made beforehand, without any involvement of national parliaments or the European Parliament or broader public scrutiny or discussion.

The same is true of the VIS, as the Commission only proposed formal legislation to establish the details of this system in December 2004. At least the Commission carried out an impact assessment for the VIS. Again, as pointed out above, there was no such assessment carried out before deciding to spend considerable sums on establishing SIS II.

***The current SIS provisions***

The key issues arising from any database are the types of data kept, the grounds for keeping the data, the persons who have access to the data (and on what grounds), and the data protection rights of individuals. For the current SIS, the categories of data which can be kept are set out in Article 94 of the Schengen Convention. The grounds for keeping the data are known as 'alerts', and Articles 95-100 of the Convention allow for six types of alert, concerning: extradition (Article 95); denial of entry to the Schengen states (Article 96); missing persons or persons needing protection (Article 97); persons wanted in a judicial procedure (Article 98); persons or objects to be placed under surveillance (Article 99) and objects wanted for seizure or evidence (Article 100). The persons with access to SIS data, before the amendments of 2004 and 2005, are the police, customs and border control authorities, along with (for immigration data) the visa and immigration authorities (Article 101). Data protection provisions are set out in Articles 109-112 and 114-115 of the Convention, described further below. There are also other data processing issues concerning the SIS, in particular the issue of 'flagging' alerts (preventing any action based on the alert from being carried out on a particular Member State's territory), and the question of how long the alerts are kept in the database (Articles 112-113 of the Schengen Convention address this).

The 2004 Regulation on the SIS set out eight amendments to the SIS rules, amending Articles 92, 94, 101 (twice), 102 and 103 of the Convention, and inserted new Articles 112a and 113a. The parallel 2005 third-pillar Decision set out thirteen amendments, amending Articles 92, 94 (twice), 99 (three times), 100, 101, 103 and 113 of the Convention, and inserting new Articles 101a, 101b, 112a and 113a. Six of the amendments set out in these two measures overlap; so taken together, they make fifteen amendments to the Schengen rules. The

2005 Regulation on access to SIS data by vehicle registration authorities simply adds an Article 102a to the Convention.

The content and status of these amendments is as follows:

a) the amendment to Article 92 provides expressly for the existence of the Sirene system; it applies from 13 June 2005;
b) the first amendment to Article 94 permits vehicles, not just objects, to be the subject of surveillance in accordance with Article 99; the date of its entry into force has not yet been fixed;
c) the second amendment to Article 94 amends the categories of personal data to be included on the SIS to add all forenames (not just the initials of middle names) plus an indication of whether a person has escaped and the type of offence committed by persons wanted for extradition; the date of its entry into force has not yet been fixed;
d) the first amendment to Article 99 extends the scope of that Article to include boats, aircraft and containers (Article 99(1)); the date of its entry into force has not yet been fixed;
e) the second amendment to Article 99 allows the security services to place the names of persons into the SIS without prior consultation of other Member States (Article 99(3)); it applies from 13 June 2005;
f) the third amendment to Article 99 allows for searches of boats, aircraft and containers (Article 99(5)); the date of its entry into force has not yet been fixed;
g) the amendment to Article 100 expands the list of objects which can be listed in the SIS; the date of its entry into force has not yet been fixed;
h) the first amendment to Article 101 allows judicial authorities to have access to SIS data; it applies from 13 June 2005;
i) the second amendment to Article 101 allows visa and immigration authorities to access data on stolen travel documents; the date of its entry into force has not yet been fixed;
j) an amendment inserts new Articles 101a and 101b into the Convention, giving authority to Europol and the national members of Eurojust respectively to search Article 95, 99 and 100 data (in the case of Europol) and Articles 95 and 98 (Eurojust); the date of this amendment's entry into force (which may take place at separate times for Europol and Eurojust) has not yet been fixed;
k) an amendment to Article 102 follows from the second amendment to Article 101; the date of its entry into force has not yet been fixed;
l) the new Article 102a, giving access to data on vehicles to vehicle registration authorities, will apply six months after publication of the 2005 Regulation, so likely in December 2005;
m) an amendment to Article 103 requires all data transmissions to be recorded, not just one-tenth of them; the date of its entry into force has not yet been fixed, but 1 January 2006 has been suggested by the Council Presidency (in Council doc. 8586/05);
n) a new Article 112a sets out conservation periods for personal Sirene data; it applies from 11 September 2005;
o) an amendment to Article 113 changes the rules governing time periods for conservation of data concerning objects to a 10-year maximum, with a 5-five year maximum for objects listed pursuant to Article 99 (the

rules currently permit a 10-year norm for objects, with five years for identity documents and banknotes and three years for vehicles, caravans and trailers); the date of its entry into force has not yet been fixed; and

p) a new Article 113a sets out conservation periods for non-personal Sirene data; it applies from 11 September 2005.

**The new proposals: analysis and critique**

***Overview of the new proposals***

Two of the three proposals (the Regulation on immigration data and the Decision on policing/criminal law data) go into great detail about the functioning of SIS II. In fact, much of their text overlaps. This is apparently believed to be necessary by the Commission because SIS II, like the current SIS, will perform a dual function as regards immigration control on the one hand (an EC law issue) and policing and criminal law on the other (an EU law issue). The third measure, a proposed Regulation based on the EC's transport law powers, simply provides for access by vehicle registration authorities to SIS data on stolen vehicles. It would replace the recent Regulation on access to SIS data by these authorities, but in fact would be identical to the text of that Regulation.

A fundamental problem with the Commission's proposals is the lack of any detailed explanatory commentary on the text. This makes it difficult to discern what the Commission's objectives are with the proposals.

The immigration Regulation and the policing and criminal law Decision have the following structure:

a) Chapter I of each measure (Articles 1-5), sets out general provisions dealing with objectives, definitions, basic structure and costs; these provisions of the Regulation and Decision are essentially identical (except for some additional definitions in the Regulation, notably excluding family members of EU citizens exercising free movement rights and persons covered by EC treaties with non-EU states on free movement of persons from the scope of the Regulation);
b) Chapter II of each measure (Articles 6-11) sets out the responsibilities of the Member States; these provisions of the Regulation and Decision are essentially identical;
c) Chapter III of each measure (Articles 12-14) sets out the responsibilities of the Commission; these provisions of the Regulation and Decision are essentially identical;
d) Chapter IV of the Regulation (Articles 15-20) sets out the key rules on the ground for issuing immigration alerts, the types of data kept, access to those alerts by various authorities and the conservation period for data; Chapters IV-VIII of the Decision, following Articles 95 and 97-100 of the current Schengen Convention, set out such key rules (except for the rules on categories of data) in turn for alerts related to: extradition and the European arrest warrant (Articles 15-22); missing persons (Articles 23-26); persons wanted for judicial procedure (Articles 27-30); persons or objects to be placed under surveillance (Articles 31-34); and objects

wanted for seizure or use as evidence in criminal proceedings (Articles 35-38);

e) Chapter V of the Regulation (Articles 21-27) and Chapter IX of the Decision (Articles 39-48) set out general data processing rules; these are identical except that the Decision sets out here the rules on categories of data (Article 39), and contains rules on the changing of alerts (Article 40(2)), 'flagging' of alerts (Article 45) and the transfer of data to third countries and international organisations (Article 48);
f) Chapter VI of the Regulation (Articles 28-31) and Chapter X of the Decision (Articles 49-53) set out data protection rules; these are identical except for certain differences explained below;
g) Chapter VII of the Regulation (Articles 32-33) and Chapter XI of the Decision (Articles 54-55) set out rules concerning liability and sanctions; these provisions are identical;
h) Chapter XII of the Decision (Articles 56-58) sets out specific rules on access to data by Europol and Eurojust; it has no parallel in the Regulation; and
i) finally, Chapter VIII of the Regulation (Articles 34-39) and Chapter of the Decision (Articles 59-65) set out final rules, concerning monitoring and evaluation, repeal of parts of the Schengen acquis and EC/EU legislation on the Sirene manual, transitional provisions and the date of entry into force; these provisions are essentially identical.

***General changes***

Several general points arising from the proposed measures should be considered first. The three measures, will, between them, replace all of the current provisions of the Schengen Convention dealing with the SIS, along with nine relevant Executive Committee decisions (including the decision establishing the Sirene manual) and two EC/EU measures concerning amendment of the Sirene manual.

Next, the Commission suggests that it should be responsible for the operational management of the SIS, a role it has already for Eurodac and has proposed for itself as regards the VIS. The Commission would also have an extensive role adopting measures implementing the SIS legislation, controlled by a committee of Member States' representatives who would have to support draft Commission measures by a qualified majority vote. Furthermore, the costs of the SIS at EU level would be charged to the EC budget.

As regards data protection, the immigration data Regulation would be governed by the EC's data protection directive (as regards the national application of the SIS) as well as Regulation 45/2001, which sets out similar rules governing data protection as regards data processed by the EU institutions, including a role for a European Data protection supervisor. On the other hand, the Decision would not be governed by the EC Directive, although it would be subject to the EC data protection Regulation, including the role of the European Data Protection Supervisor. The Decision would also be subject to the Council of Europe's data protection Convention (Article 49); at present all the SIS provisions are subject to this Convention and a Council of Europe recommendation on the processing of police data (Article 117 of the Schengen Convention).

Finally, since immigration data in the SIS would be governed by an EC Regulation, rather than a Convention allocated to the third pillar, it would be clear that the rules on this issue were directly applicable in national legal systems; the Regulation would also be enforceable by infringement actions brought by the Commission and the final national courts in all Member States applying the Regulation could send references to the Court of Justice on the interpretation or validity of the Regulation. Individuals could also sue the Commission directly regarding the Regulation if it is interpreted to mean that the Commission, when managing the SIS, must respond to requests for access to data. On the other hand, the Decision would remain subject to the current judicial rules applying to the Schengen Convention SIS provisions. These rules only allow for references from national courts to the Court of Justice to the extent that Member States have opted in to this jurisdiction (thirteen Member States have), as well as jurisdiction for the Court to settle disputes between Member States. There is no express jurisdiction to hear disputes brought by individuals suing the Commission directly.

### *Data protection rights*

#### *Existing rules*

The first specific issue to consider regarding the proposals is whether individual data protection rights would be enhanced. At present, the Schengen Convention provides that the right of persons to have access to SIS data concerning them will be exercised according to the national law where they invoke that right (Article 109(1)). Communication of the data may be refused if indispensable for the performance of a task connected to the alert or to protect the rights and freedoms of others; it shall always be refused if a person is under surveillance (Article 109(2)). National law may provide that a national supervisory authority shall decide on whether and how the requested information will be communicated (Article 109(1)). If the data was inserted into the SIS by another Member State, it must be consulted before the data is disclosed (Article 109(1)).

Article 110 of the Convention provides that any person may have factually inaccurate information corrected or unlawfully stored information deleted. Of course, the ability to make arguments on this point is dependent upon successfully invoking the right to access to the information in the first plan. Article 111 then provides that any person may bring an administrative or judicial claim in a Member State to correct or delete information, to gain access to it, or to obtain compensation; Member States agree to recognise the relevant judgments or administrative decisions.

Article 114 obliges Member States to set up national data protection authorities with the power to supervise the national data files of the SIS and to check that the processing and use of the data does not violate individual rights. Any person has the right to request the supervisory authority to check their data in the SIS and the use made of it, but this right is governed by the relevant national law. If the data were entered by another Member State, the relevant supervisory authorities shall work closely together. Article 115 establishes a Joint Supervisory Authority, which shall supervise the technical support

function of the SIS. It shall also examine difficulties of interpretation or application regarding the system, or problems that may occur regarding national supervisory authorities' supervision or exercise of the right to access, and for drawing up proposed harmonised solutions to joint problems.

Article 116 allocates liability among Member States for wrongful data or illegal use of data. Finally, Article 117 requires Member States to maintain data protection standards in accordance with the Council of Europe Convention on data protection and a Council of Europe recommendation on the use of data in the police sector. There is no express provision concerning the transfer of data to third states or international organisations (setting aside the recent addition of provisions concerning SIS access for Europol and Eurojust).

***Proposed new rules***

Starting with the proposed Regulation on SIS immigration data, the first relevant new provision is Article 15(3), which gives individuals a right to review or appeal of a decision to issue an alert in the first place. This is a new right as compared to the existing Schengen rules and is obviously welcome. But this provision does not expressly require a person to be informed when an alert is issued, or when an alert is used in order to take decisions. Although the existing rules on border control require authorities to tell persons if they have been refused entry because their name is in the SIS, other existing rules on visas and residence permits do not contain equivalent provisions. The point would be even more important under the proposed Regulation, since SIS data would be used for more immigration (and asylum) purposes. Moreover, if a person is not informed of an alert when it is initially issued, it may be more difficult to determine which Member State issued the alert, and so more difficult in practice to challenge its use or validity later on. Also there are no details regarding the review or appeal, such as the right to be informed of how to make it, to have legal assistance, or to have suspensory effect of an appeal; and there are no provisions on the remedy following a successful challenge.

Next, Article 28 of the Regulation gives individuals a right to information on five issues: the identity of the data controller; the purposes for processing data; the potential recipients of the data; the reason for issuing the alert; and the existence of the right of data access and rectification. These are new rights not expressly set out in the current Convention and are welcome. In particular, the obligation to inform persons of the identity of the data controller must mean that the individual is informed of which Member State issued the alert. However, there is no reference to an obligation to inform individuals about the national or EU supervisory authorities, the right of erasure of data, or the mechanisms of making a challenge, including relevant remedies. Also, it is not clear when the obligations set out in Article 28 have to be carried out, in the absence of an express obligation to inform individuals as soon as an alert concerning them is entered into the SIS or used to take a decision.

Article 29(1) then provides that the rights of access, erasure or rectification shall be exercised in accordance with the law of the Member State in which that access is invoked. The current provision stating that communication of the data may be refused if indispensable for the performance of a task connected

to the alert or to protect the rights and freedoms of others does not appear. Nor does the current provision stating that national law may provide that a national supervisory authority shall decide on whether and how the requested information will be communicated. However, the current provision for consultation between Member States if the data was inserted into the SIS by another Member State is retained (Article 29(2)), with further elaboration on the procedures for consultation. New provisions state that the data must be communicated as soon as possible, with a 60-day maximum (Article 29(3)), and that information about the follow-up to an application for rectification or erasure must be communicated within six months (Article 29(4)).

The deletion of the current proviso permitting denial of the right of access is an essential and highly welcome change, as are the two new provisions setting deadlines for action by Member States. Nevertheless, the provisions are still weakened by the absence of a requirement to inform persons that an alert concerning them has been issued in the first place and that the alert has been used to take a decision.

Article 30 of the Regulation provides that there is a right to bring actions before the courts as regards the rights of access, information, erasure, rectification or compensation for any person in the territory of a Member State. The reference to bringing actions before an administrative body is deleted, as is the obligation of Member States to recognise each other's judgments. The deletion of the latter point is unfortunate as such an obligation could prove useful in practice. It would have been preferable to delete the territorial limitation placed on access to court, since obviously many persons with complaints about use of SIS immigration data will not be on the territory of a Member State. Indeed, the whole point is that if it were not for the inaccurate data contained in the SIS, the individual concerned usually *would* be on the territory of a Member State; so the requirement to be on the territory to access the courts is simply absurd.

Article 31(1) of the Regulation contains the current obligations as regards national data protection authorities, with the absence of the provisions that such authorities should have the power to check the national data files and the role of ensuring that the processing and use of data does not violate data subjects' rights. The individual right to ask the supervisory authority to check the data has been dropped. There seems to be no convincing reason to make any of these changes, particularly the omission of the right to ask to supervisory authority to check the data. Finally, Article 31(2) specifies that the European Data Protection Supervisor, rather than the existing Joint Supervisory Authority, shall monitor the Commission's application of the Regulation. Unfortunately the current powers of the joint supervisory authority to examine difficulties of interpretation or application and national supervisory authorities' supervision or exercise of the right to access, and to draw up proposed solutions to problems, are not mentioned.

Again, the Regulation, like the current rules, contains no express provision on the transfer of data to third states or international organisations.

Since, according to the preamble to the Regulation, the EC data protection directive applies to national authorities acting within the scope of the Regulation, and the EC data protection Regulation applies to the Commission, it is necessary to consider this other legislation. As for the Directive, Article 13 permits Member States to impose various restrictions on key data protection rights; does it apply to the Regulation? If so, then the deletion of the specific clause in the Schengen Convention on restriction of data access would be purely a formality, since Member States would retain the power to restrict access. Article 22 of the Directive provides for a right to access national courts with no reference to any territorial limitation; so there is a conflict on this point between the Directive and the proposed Regulation. Articles 25 and 26 of the Directive provide for a detailed and controversial regime governing the transfers of data to third countries; the interpretation of these provisions is at issue in the pending legal challenges by the EP to the Council's and Commission's approval of the transfer of passenger data to the USA.

If these three provisions of the Directive apply to the Regulation, this means that there will still be extensive powers for Member States to restrict the right of information and the right of access to data, and there will be extensive possibilities to transfer SIS data to third countries, if the Commission's and Council's interpretation of the external relations rules in the passenger data dispute is correct. The Regulation would moreover reduce the right of access to court found in the Regulation (assuming such a restriction is valid). So the data protection rules would be similar or even worse that the current Schengen rules on SIS data protection.

But one apparent improvement on those current rules can be found in Article 28 of the Directive, on the role of national data protection supervisory authorities, which provides in part as follows:

> 3. Each authority shall in particular be endowed with:
>
> - investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
> - effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
> - the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.
> Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.
>
> 4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.
> Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions

adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

If these powers apply fully to the data exchanged under the proposed Regulation, then there is no ground to complain about the provisions on this issue omitted from the Regulation, because the Directive clearly gives the national data protection authorities considerable powers. This should be welcomed, although it is not clear if Member States must give these authorities the power to block, erase or destroy data in all cases.

As for the Regulation on data processing by the EC institutions, the relevant provisions are essentially the same as those under the Directive. However, since Articles 28-30 of the proposed SIS Regulation only refer to Member States, it is not clear whether disputes relating to SIS II immigration data could be brought directly against the Commission (and subsequently directly before the EC courts or the European Data Protection Supervisor).

As for the proposed third pillar Decision on the SIS, it is identical to the proposal Regulation, apart from the following:

a) the Council of Europe data protection Convention applies (Article 49 of the Regulation); this maintains the current Schengen Convention provision;
b) there is a provision allowing refusal of the right of information, if it would impede the authorities' tasks; this reflects the restriction on right of access found in the current Schengen Convention (Article 49(2));
c) there is a provision allowing refusal of the right of access, carried forward without amendment from the restriction currently found in the Schengen Convention (Article 51(4));
d) the Decision maintains the current rule allowing the individual to ask the national supervisory authority to check that the data processing regarding him is lawful (Article 53(1));
e) there is an express reference to the role of the Europol and Eurojust supervisory authority (Article 53(2)); and
f) the transfer of data to third countries or international organisations is expressly permitted, if the body concerned has an agreement with the EU and maintains a adequate level of protection (Article 48).

The distinctions between the Decision and the Regulation essentially reflect provisions found in the EC data protection Directive regarding derogations from data protection rights (points (b) and (c) above), the role of national supervisory authorities (point (d) above), and the transfer of data outside the EU (point (e) above). If the provisions on these points in the EC Directive are taken to apply to the proposed Regulation, and if the European Data Protection Supervisor can apply all his powers in the EC data protection Regulation to the Commission when it applies the Decision (both points as discussed above), then there is in fact little to distinguish the two proposals, except that the extensive powers which national data protection authorities are supposed to possess under the Directive will not apply to the Decision.

A better model for data protection rights can be found in the Commission's recent proposal for the VIS, which provides in part (Article 31):

> 5. If the Member State responsible does not agree that data recorded in the VIS is inaccurate or has been recorded unlawfully, it shall explain in writing to the person concerned without delay why it is not prepared to correct or delete data relating to him.
>
> 6. The Member State responsible shall also provide the person concerned with information explaining the steps which he can take if he does not accept the explanation provided. This shall include information on how to bring an action or a complaint before the competent authorities or courts of that Member State and any financial or other assistance that is available in accordance with the laws, regulations and procedures of that Member State.

Article 32 of this proposal also provides for cooperation between and assistance of national supervisory authorities, while Article 33 does not appear to require presence on the territory in order to bring disputes to court. But again it is not clear whether the data protection Directive's rules on exemptions from data protection rights, external transfers or extended powers of national data protection authorities apply, or whether complaints can be made by individuals against the Commission to the courts or the European Data Protection Supervisor. Also, there is no express right of appeal in this proposal against the decision to place data into the VIS.

***Types of alerts/categories of data***

There are no new types of alerts proposed in either the proposed Regulation or Decision. However, there are proposed changes to two of the types of alerts. The first change concerns alerts on immigration data. At present, the grounds for inclusion of this data (Article 96 of the Schengen Convention) are that the decision 'may be based on a threat to public policy or public security or to national security which the presence of an alien in national territory may pose'. This may arise 'in particular' in the case of an alien 'convicted of an offence carrying a penalty involving deprivation of liberty of at least one year' or where there are 'serious grounds for believing that [the person] has committed serious criminal offences' or 'clear evidence of an intention to commit such offences' on a Member State's territory. An alert 'may' also be based on an expulsion order or similar measure 'based on a failure to comply with' national immigration law.

The proposed revised grounds for an alert in Article15 of the proposed Regulation are first, a 'serious' threat to public policy or public security (no reference to national security), 'based on an individual assessment', 'in particular' if the person concerned has been sentenced to a penalty of over one year following conviction for an offence referred to in the list of thirty-two offences set out in the European Arrest Warrant, or is on an EU foreign policy list of persons to be banned from entry. Also, an alert could be issued if a person is subject to a re-entry ban in accordance with the EC's directive on expulsion – but the proposal for this Directive has not yet been issued by the Commission. The alerts shall be issued 'without prejudice' to a more favourable provision of specified EC immigration and asylum legislation.

It should also be kept in mind that the family members of EU citizens exercising free movement rights are exempt from the proposed Regulation, unlike the present position, although the Commission has long argued that such persons must be considered exempt from inclusion pursuant to Article 96 of the Schengen Convention already because this would breach EC free movement law. The Opinion of an Advocate-General in a pending legal challenge backs the Commission's position (Opinion in Case C-503/03 *Commission* v *Spain*).

There are specific provisions to deal with cases where persons gain citizenship of a Member State or the status of family member (Article 20(2) and (3)), and also a review to determine whether the alert should be maintained when a person becomes covered by the EC immigration legislation which could trump the alerts.

It is certainly welcome that the proposed Regulation clarifies the position regarding family members of EU citizens, although the Court of Justice may reach the same conclusion shortly regarding the current system. It is also useful to provide for a system of deleting the alerts when the situation changes. But these provisions do not go far enough, as they should also provide for 'trumping' the SIS when a person gains status under the EC temporary protection Directive, or a relevant association agreement (particularly the agreement with Turkey, which provides for protection from expulsion for Turkish workers and their family members). Furthermore, the provisions on reviewing the alerts do not allow for review of the alert in the process of making a decision on initial residence status. Such a decision would presumably still be governed by Article 25(1) of the Schengen Convention, which in principle bans a residence permit from being issued to a person on the SIS. This provision overlaps with Articles 15 and 20 of the proposed Regulation and so should obviously be reconsidered as well.

As for the criteria for inclusion, it is not clear if the two categories listed in the proposed Regulation are non-exhaustive, or whether data can be inserted on other grounds. From the case law of the European Court of Human Rights, it is clear that imprecise provisions concerning the grounds on which authorities can store personal data breach the right to privacy protected by the European Convention of Human Rights because individuals are unable to find out what rules apply to the collection and use of their personal data. At least the threshold for including data on public policy or public security grounds has been raised in several respects requiring a prior assessment, a serious threat, and a *sentence* of one year (also dropping the idea of listing persons on national security grounds), although the two grounds for listing persons here clearly appear to be non-exhaustive. It is impossible to judge the proposed ground for listing people by reference to the EC's expulsion directive, in the absence of the proposed text of that Directive (!).

The second change concerns alerts relating to extradition data. The proposed Decision would expand the scope of these alerts to include requests for execution of a European Arrest Warrant, and will also provide for inclusion of data related to the warrant or the extradition request in the SIS (Articles 15-17 of the proposed Decision).

The third change would be the inclusion of data related to misused identity (Article 44 of the Decision and Article 25 of the Regulation). This would be a useful addition to the system because it will reduce the number of cases where persons are wrongly identified as the object of an alert.

As for categories of data, there are several important changes compared to Article 94 of the Schengen Convention, as amended by the 2004 Regulation and 2005 Decision. In particular (according to Article 16 of the proposed Regulation and Article 39 of the proposed Decision), fingerprints and photographs could be included in the SIS, along with the person's name at birth, previously used names, the authority issuing the alert, and links to other alerts (a point discussed further below). The current provision banning the inclusion of any other information, particularly sensitive information as defined in the Council of Europe's data protection Convention, would be dropped. The proposed Regulation differs slightly from the proposed Decision in that data concerning the decision on expulsion could also be included, but not a reference to reasons for the alert (although the reasons would presumably be set out in the expulsion decision), the actions to be taken (although this could be considered obvious), and whether the person concerned is armed, violent or has escaped.

As pointed out in the recent Statewatch report on SIS II plans, the inclusion of fingerprint and photograph information would in effect turn the SIS into a law enforcement tool, particularly if combined with the VIS, Eurodac and Europol's planned information system (all issues expressly on the EU's agenda). The risks resulting from wrongful identification, access or use of such data have not been thought through.

***Access by authorities***

At present, police and border control authorities have access to all SIS data. Also, Article 96 data is available to authorities deciding on visas and residence permits. Judicial authorities will be granted access to all SIS data according to the relevant provisions of the 2004 Regulation and the 2005 Decision, from 13 June 2005. Furthermore, in accordance with the same legislation, the visa and residence permit authorities will have access to data on stolen travel documents, Europol will have access to Article 95, 97 and 99 data, and Eurojust's national members will have access to Article 95 and 98 data, at a date to be determined. Finally, vehicle registration authorities will have access to stolen vehicle data from December 2005, according to the recent Regulation on this issue.

The proposed new Regulation on immigration data in the SIS would extend access to that data to asylum authorities, in order to determine the Member State with responsibility for asylum applications on the grounds of an illegal stay (Article 18(2) of the proposal), and to take decisions on the asylum claim, on the grounds that a person is a threat to public order or internal security (Article 18(3)). It would also extend access to the same data to the authorities involved with expulsion, in order to assist identification of persons (Article 18(1) of the proposal). But police would no longer have access to immigration data (Article 17).

The proposed Decision on police and criminal law data would retain the existing access rules for various national agencies, as well as Europol. Eurojust staff members would have access in their own capacity, rather than only via the national members of Eurojust (Article 58 of the proposal). As for the additional data relating to extradition and European arrest warrants, only Eurojust and the national judicial authorities can access it (Articles 16 and 17 of the proposal). Otherwise the conditions for Europol and Eurojust to have access to data are essentially the same as those in the 2005 Decision.

The problem here is with the extension of access to immigration data, especially to asylum authorities. In order to apply the Dublin Regulation to determine which Member State is responsible for an asylum application, national authorities need precise information and evidence that a person has been illegally staying on a territory for a specific time. A mere listing in the SIS cannot provide that information. Also, the question of whether a person can be excluded from refugee status is an issue requiring detailed analysis, which according to refugee law (including the EC's asylum legislation) applies a different test from whether a person represents a 'threat to public order or internal security'. A listing in the SIS in accordance with Article 15(1)(a) of the Regulation is manifestly insufficient to this end, particularly since this provision appears to set out non-exhaustive grounds for listing persons.

***Data processing rules***

The key changes here concerning the linking of alerts and the rules on conservation of data. On the first point, Article 26 of the Regulation and Article 46 of the Decision permit linking of different alerts, a prospect not permitted by the current SIS. The recent Statewatch report on the SIS II plans raised a number of concerns about this idea.

On the second point, the current period of conservation of data is (as regards personal data) to keep the data in the SIS only for the time required. There must be a review after three years at a maximum, or a one year maximum for personal data kept for surveillance purposes. But Member States may decide during the review period to keep the data in the system (Article 112 of the Convention)). As for non-personal data, the current rules (Article 113 of the Convention) permit it to be kept for 10 years, but data on identity cards or banknotes for 5 years, and data on vehicles, trailers and caravans for 3 years. These periods are amended by the 2005 Decision so that a 10 year maximum still applies, with the sole exception a 5 year maximum for data concerning surveillance of objects.

The proposed immigration Regulation (Article 20) would schedule automatic deletion of data after five years, but a Member State could elect to maintain the alert before this period expired. The policing and criminal law Decision would permit extradition and arrest warrant data to be kept for 10 years, again with the power for Member States to decide to maintain the alerts (Article 19 of the proposal). But the alert would expire earlier if the person concerned were surrendered or extradited, or if the validity of the warrant expires. The same time period would apply to data on missing persons or persons to be

placed under protection, except for an earlier expiry of the alert once a person is placed under protection (Article 25), and for data on persons wanted for judicial procedures (Article 29) except for an earlier expiry of the alert once the residence or domicile of person has been found. As for data on surveillance (Article 34), the inclusion of personal data would have to be reviewed after three years, instead of one year, and the inclusion of data on objects after five years. The latter time period is the same as the current rules following their amendment by the 2005 Decision, except that there would be a possibility to extend the inclusion of this data in the SIS after the deadline. Finally, data on missing objects (Article 38) retain a three year review period for personal data, with a 10 year review period for all non-personal data as at present. But again the prospect of a possible extension after ten years would be new. There would be an earlier deletion of the data if the object is seized.

In conclusion, it can be seen that for every type of alert, the time period for keeping the data in the SIS would be extended (from 3 to 5 years for immigration data; from 3 to 10 years for data on extradition, missing persons and persons wanted for a judicial procedure; from 1 to 3 years for surveillance of persons; and possible extensions for the first time after the 5 or 10 year maxima for data on objects). The Commission does not put forward any rationale for this.

***Sources**: Schengen acquis: OJ 2000 L 239; Sirene manual: OJ 2003 C 38; Regulation on development of SIS II: OJ 2001 L 328; Decision on development of SIS II: OJ 2001 L 328; Regulation 871/2004 amending Schengen SIS rules for immigration data OJ 2004 L 162; Decision 2005/811 amending Schengen SIS rules for policing and criminal law data OJ 2005 L 68; Regulation on Sirene manual amendment: OJ 2001 L 328; Decision on Sirene manual amendment: OJ 2001 L 328; 2005 Regulation on access to SIS data by vehicle registration authorities: OJ 2005 C 111 E 2005 proposals: COM (2005) 230 (third pillar Decision); COM (2005) 236 (immigration data Regulation); COM (2005) 237 (vehicle registration Regulation); Council conclusions on SIS functions: 2002, 2003 2004; Statewatch report on SIS II plans (May 2005).*

Professor Steve Peers, University of Essex
June 2005