CEPS Paper in
LIBERTY and SECURITY in Europe

Justice and Home Affairs Databases and a Smart Borders System at EU External Borders

An Evaluation of Current and Forthcoming Proposals

Didier Bigo, Sergio Carrera, Ben Hayes, Nicholas Hernanz and Julien Jeandesboz

No. 52/December 2012

Abstract

This study examines current and forthcoming measures related to the exchange of data and information in EU Justice and Home Affairs policies, with a focus on the 'smart borders' initiative. It argues that there is no reversibility in the growing reliance on such schemes and asks whether current and forthcoming proposals are necessary and original. It outlines the main challenges raised by the proposals, including issues related to the right to data protection, but also to privacy and non-discrimination.

This study was originally commissioned by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and is available for free downloading on its website at http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79693 It is republished on the CEPS website with the kind permission of the European Parliament. Research for this study was jointly coordinated by the Centre d'Etudes sur les Conflits (C&C) and the Justice and Home Affairs section of the Centre for European Policy Studies (CEPS).

ISBN 978-94-6138-258-0
Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

List of Abbreviations

ABC	Automatic Border Control
AFSJ	Area of Freedom, Security and Justice
AMF	Asylum and Migration Fund
API	Advanced Passenger Information
AWF	Analytical Work Files
BMS	Biometric Matching System
CEPOL	European Police College
CJEU	Court of Justice of the European Union
CIS	Customs Information System
CMS	Case Management System
CoE	Council of Europe
CT	Counter-Terrorism
DG	Directorate-General
DHS	Department of Homeland Security (US)
ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EIS	Europol Information System
EIXM	European Information Exchange Model
ESTA	European System of Travel Authorisation
EU	European Union
EUROSUR	European Border Surveillance System
FIS	Frontex Information System
FP7	Seventh Framework Programme (European Commission)
GAO	Government Accountability Office (US)
IMS	Information Management Strategy
ISF	Internal Security Fund
ISS	EU Internal Security Strategy
IT	Information Technology
JHA	Justice and Home Affairs
LIBE	Committee on Civil Liberties, Justice and Home Affairs (EP)
MS	Member State

NAFTA	North-American Free Trade Area
OCTA	Organised Crime Threat Assessment
OLAF	European Anti-Fraud Office
PNR	Passenger Name Record
RTP	Registered Travellers Programme
SBC	Schengen Borders Code
SIENA	Secure Information Network Application (Europol)
SIS	Schengen Information System
SOA	Service-Oriented Architecture
SOC	Serious and Organised Crime
SOCTA	Serious and Organised Crime Threat Assessment
STOA	Science and Technology Options Assessment
TCN	Third-country nationals
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Programme (US)
TFTS	Terrorist Finance Tracking System (EU)
US	United States
VIS	Visa Information System

Executive Summary

This study argues that there is **no reversibility** in the growing reliance on data and information exchange schemes for the conduct of the European Union's justice and home affairs (JHA) policies. The question of whether or not past policy options are reversible has indeed become central in the debates surrounding this policy domain, which have been characterised over the past few years by a steady flow of proposals aiming at establishing new, large-scale systems for law enforcement purposes. It surfaces very strongly in view of the forthcoming legislative proposals on the 2011 'smart borders' initiative, to be tabled by the European Commission in December 2012, but also when considering the broader landscape of EU Justice and Home Affairs databases, of which 'smart borders' will be part. 'Smart borders' consists of two data and information exchange schemes: the Entry/Exit System (EES) and the Registered Traveller Programme (RTP). JHA databases and 'smart borders' **are usually not considered jointly,** in the name of the separateness between EU policy domains falling under the rubric of the Area of Freedom, Security and Justice (AFSJ) – here, police and justice cooperation – on the one hand, and external border control on the other.

In **Section 2**, the study suggests that the **continuous expansion of data and information exchange schemes in the context of EU AFSJ policies calls this separateness into question**. Over the past decade, an increasingly dense landscape of data and information exchange schemes has grown out of EU activities. In an overview of what it called 'information management' in the EU published in 2010, the European Commission identified 25 such schemes, most of them decided and implemented over the past ten years, with more being either considered or in development. What is striking about this landscape is the way in which each new initiative is framed as a necessary measure **to 'fill the gaps' or 'connect the dots'** in the data and information that national and EU law enforcement agencies, bodies and services can use. The questions raised by the 'smart borders' initiative have to be understood in relation to this broader trend and to the principles on which it unfolds.

In **Section 3**, the study asks whether 'smart borders' are actually about what happens at the external, territorial borders of the Member States of the EU. The EES and the RTP are mostly about what happens before and after the border. In conjunction with the Visa Information System (VIS) and the Schengen Information System (SIS, and its would-be successor SIS II), they foresee the establishment of pre- and post-border screening procedures targeting all foreign visitors to the EU. Associated with other data and information systems, they **destabilise the foreigner/citizen divide** and lay down the conditions for the proactive monitoring and sorting of large numbers of persons.

In **Section 4**, the study asks whether the impact of smart borders, associated with other initiatives on 'JHA databases', should be exclusively understood in terms of data protection. Matters related to 'JHA databases' might be technical, but the questions they raise touch upon key legal and political issues. In this sense, the **legal challenge related to the right to data protection** cannot be overlooked. This legal challenge is embodied in the necessary debate surrounding the establishment of JHA databases, which lies at the heart of the proportionality principle test. Observing the requirements following from the right to data protection is necessary, but it should **not be regarded as sufficient for justifying new data and information exchange schemes**. The monitoring and sorting of large numbers of persons bear the potential for significant social harm. A particular challenge in this respect is non-discrimination, and the way in which the growing landscape of EU data and information exchange schemes can generate **statistical discrimination**.

KEY FINDINGS

- The key questions involved in the discussion of JHA databases and 'smart borders' are reversibility, necessity and originality.
- The impact of current and forthcoming measures in these areas should not only be discussed in relation to the right to data protection. Key challenges include the right to privacy and non-discrimination.
- There is no clear definition of a 'JHA database'.
- Existing knowledge on JHA data and information exchange schemes highlights the absence of a regular effort at consolidating a detailed picture of all data and information exchange in the field of justice and home affairs, across measures and policy domains. The distinction between centralised and decentralised systems among JHA databases is misleading.
- The EU JHA database landscape involves distributed systems, which does not mean that there is a structural guarantee that data and information exchanges are compartmentalised. Among these distributed systems, the distinction between personal and non-personal data is increasingly replaced by the distinction between personal and operational data, the latter involving 'anonymised' or 'depersonalised' data. The maintenance of this distinction depends on the capacity of law-enforcement agencies to effectively depersonalise data, which raises issues related to the right to data protection and beyond, to privacy and non-discrimination.
- The main trend in the EU landscape of JHA databases is towards multi-purpose data and information schemes, in the context of a growing convergence towards law-enforcement as intelligence rather than criminal investigation. This trend is nurtured by the focus on 'information management', understood as the promotion of information-sharing by default, availability and interoperability.
- In this context, EU agencies and bodies have increasingly become data processors in their own right, and are confronted with the implications of the abovementioned trends. Activities linked to the management of large-scale IT systems should also be addressed in this regard, insofar as management seems to include the monitoring of research and the steering of pilot schemes to develop further JHA databases.
- Current and forthcoming proposals, especially the EU PNR (Passenger Name Record) and EU TFTS (Terrorist Finance and Tracking System) initiatives, raise the questions of mass data processing for law-enforcement purposes, automated data processing and profiling as potential future trends with regard to JHA databases.
- The 'smart borders' initiative aims at supplementing the SIS and VIS by logging movements in and out of the Schengen area (Entry/Exit System) and facilitating fast-track entry for pre-vetted registered travellers (Registered Traveller Programme). The degree to which 'smart borders' is the inevitable outcome of existing EU policies on external border control, migration and visas can however be challenged, considering the track record of these measures and the change in scope, purpose and costs that they have experienced over the past decade.
- The 'smart borders' system is no longer only and mainly about borders: It involve the surveillance of foreigners travelling to, within and out of the Union.
- The planned 'Entry-Exit System' will lead to the fingerprinting of *all* third-country nationals entering the European Union, significantly expanding the EU's biometric information systems and increasing the amount of personal data accessible to law enforcement and security agencies.

- The planned 'Registered Traveller Programme', under which business and other frequent travellers would benefit from faster crossings, will institutionalise a two-tier border control system in the EU based on crude indicators such as wealth, nationality, employer and travel history. In envisaging the gradual replacement of border guards with 'Automated Border Control' gates, the planned 'smart borders' proposals may also pave the way for increased surveillance of EU citizens, whose movements could easily be recorded and stored in future.
- The proposed European Border Surveillance System (EUROSUR) is the most ambitious surveillance system ever envisaged by the EU with important implications for the protection of fundamental rights and democratic control, which should be assessed in the same way as other 'smart border' proposals.
- The first legal challenge posed by JHA databases relates to the principle and fundamental right of privacy. Independently from the personal character of the information collected and/or processed, databases are in tension with the general EU principle of privacy, which extends beyond data protection to the wider right to private life as envisaged in the Charter and also includes 'anonymised' or 'operational' data. The conditions under which de-personalised data can or could be re-personalised by law enforcement authorities are of utmost relevance.
- JHA databases have a very broad personal scope as they cover a wide range of individuals with a variety of legal statuses in accordance with EU law. This leads to a blurring of the targeted individuals as data subjects and to negative repercussions over the principle of legal certainty. They also fail to take into account the inherent vulnerability of certain groups of travellers and foreigners. Non-EU citizens can experience even more difficulties as regards the right to be informed, to access their data and to effective remedies. This risk is further increased due to the existence of multiple EU systems working on different EU AFSJ policy areas.
- An additional legal challenge pertaining to JHA databases and 'smart borders' concerns the actual necessity surrounding the establishment of JHA databases, which lies at the heart of the proportionality principle test. It is at present far from clear to which extent these systems pass satisfactorily the necessity test as applied by the European Court of Human Rights and the Court of Justice of the European Union.
- While nationality and legal status may not be considered as connecting factors for activating the EU non-discrimination system of protection for third-country nationals (TCNs), any person (independently of his/her administrative migration status) is a beneficiary of the general non-discrimination protection, which constitutes a well-established principle in the EU legal regime now expressly enshrined in Article 21 of the EU Charter. These apply equally to EU citizens and foreigners.
- It is challenging to distinguish discrimination on the basis of race and ethnic origin from that of 'nationality'. The exclusion of nationality discrimination in the scope of the Race Equality Directive is somehow at odds with a reality where discrimination of TCNs is 'multi-grounded' or multi-faceted. How can border controls be carried out in such a way that they discriminate only on grounds of nationality, and without using nationality to justify indirect discrimination on prohibited grounds?
- JHA databases and smart borders work on the basis of 'automated decision-making' parameters, which correspond to what has been denominated as 'profiling' or 'predictive data-mining'. Profiling is used to 'select' a group of people as a potential risk or a threat and may lead to discriminatory ethnic profiling, which is by nature difficult to reconcile with the obligation for national and EU law enforcement authorities and agencies not to discriminate on grounds of a sensitive nature such as national or ethnic origin.

Justice and Home Affairs Databases and a Smart Borders System at EU External Borders

An Evaluation of Current and Forthcoming Proposals

Didier Bigo, Sergio Carrera, Ben Hayes, Nicholas Hernanz and Julien Jeandesboz*

CEPS Paper in Liberty and Security in Europe No. 52
December 2012

1. Introduction

KEY FINDINGS

- The key questions involved in the discussion of JHA databases and 'smart borders' concern their reversibility, necessity and originality.
- The impact of current and forthcoming measures in these areas should not only be discussed in relation to the right to data protection. Key challenges include the right to privacy and non-discrimination.

This study argues that **there is no reversibility in the growing reliance on data and information exchange schemes for the conduct of the European Union's Justice and Home Affairs (JHA) policies.** The question of whether or not past policy options are reversible has indeed become central in the debates surrounding this policy domain, which have been characterised over the past few years by a steady flow of proposals aiming at establishing new large-scale systems for law enforcement purposes. It surfaces very strongly in the forthcoming legislative proposals on the 2011 'smart borders' initiative,[1] to be tabled by the European Commission in December 2012, but also when considering the broader landscape of EU JHA databases of which 'smart borders' will be part.

The discussion on reversibility ties in with the issue of necessity. Proposals for new data and information exchange schemes **are currently presented as necessary complements to previously adopted measures**. **To what extent can necessity be assessed in the same way for law-enforcement and security services, for the concerns of EU citizens and foreigners travelling to the EU, and for the good functioning of our democratic societies?** The concern here is legal (necessity as part of the proportionality test) and political, insofar as the reliance on data and information exchange for law-enforcement purposes can generate significant social harm. Current and forthcoming JHA databases and other initiatives such as the 'smart borders'

* Prof. Didier Bigo (Centre d'études sur les conflits, C&C), Dr Sergio Carrera (Centre for European Policy Studies, CEPS), Dr Ben Hayes (Project Director, Statewatch), Mr Nicholas Hernanz (Centre for European Policy Studies, CEPS), Dr Julien Jeandesboz (Centre d'études sur les conflits, C&C).

The authors would like to express their gratitude to Prof. Elspeth Guild (CEPS) for her comments on an earlier version of this report.

[1] European Commission (2011), *Smart borders – options and the way ahead*, COM(2011) 680 final, 25.10.2011.

system envisage a significant increase in the amount of data and information collected, exchanged and processed by law-enforcement and security services. As such, they are not only an 'upgrade' of established law-enforcement practices, but underpin their transformation – as we will show through the discussion of the 'smart borders initiative', of the territorial scope of these practices in particular. Necessity ties in with legal challenges associated with the fundamental right to data protection, but also with the general principles of privacy and non-discrimination. 'JHA databases' also raise the question of financial risks tied to the cost of these measures, and with the social and political effects associated with placing democracy under non-proportional forms of surveillance.

In this perspective, **the other issue to consider is that of originality**. Current proposals, including 'smart borders' as well as the establishment of an EU Passenger Name Record system (EU PNR) and Terrorist Finance Tracking System (TFTS) or the creation of a European Border Surveillance System (EUROSUR) take their cue from measures adopted or considered by the US government under the administration of George W. Bush and in Australia during the previous administration in office. They are also inspired by the feasibility estimates and demonstration efforts of the US and EU defence and security industry. **To what extent, however, are they reflective of the legal obligations, principles and values inscribed in the EU Treaties and other instruments composing the European legal system?** These obligations, principles and values, as section 4 will highlight, are not limited to the right to data protection, but include other issues related to their contested relationship with EU general principles of privacy and non-discrimination, which are now embodied as legally binding commitments in the EU Charter of Fundamental Rights.

1.1 Background to the discussion

The background to the present study is the question of current and forthcoming proposals on JHA databases, including the impact of the introduction of a 'smart borders' system at the external borders of the European Union. The system consists of two additional data and information exchange schemes, the Entry/Exit System (EES) and the Registered Traveller Programme (RTP). JHA databases and 'smart borders' **are usually not considered jointly, in the name of the separateness between EU policy domains** falling under the rubric of the Area of Freedom, Security and Justice (AFSJ) – here, police and justice cooperation – on the one hand, and external border control on the other. **The continuous expansion of data and information exchange schemes in the context of EU AFSJ policies** (documented in section 2), **however, calls this separateness into question**.

Over the past decade, an increasingly dense landscape of data and information exchange schemes has grown out of EU activities. We use the term 'landscape', here, to highlight that this development challenges the legal scope of rights and freedoms, as well as the traditional horizons of law-enforcement activities, which are anchored in the notion of territory. In an overview of what it called 'information management' in the EU published in 2010, the European Commission identified 25 such schemes, most of them decided and implemented over the past 10 years, with more being either considered or in development. What is striking about this landscape is the way in which each new initiative is framed as a necessary measure **to 'fill the gaps' or 'connect the dots'** in the data and information that national and EU law enforcement agencies, bodies and services can use. **The questions raised by the 'smart borders' initiative have to be understood in relation to this broader trend and to the principles on which it unfolds.**

The background to the current EU 'smart borders' initiative **should be discussed at least in part in relation to the actions undertaken by security agencies in the United States in the immediate aftermath of the attacks of 11 September 2001**. On the one hand, US agencies

began demanding advance information on foreign nationals entering the country. Initially, this data was derived from existing data collection schemes, such as passenger manifests and airline reservation databases. The situation also led, however, to the accelerated implementation of measures that had been in discussion since the mid-1990s, including a foreseen automated entry-exit system, which would ultimately be merged under the heading of the 'US-VISIT' scheme.[2] Almost all non-NAFTA (North America Free Trade Area) nationals now require pre-authorisation from the Department of Homeland Security to enter the US; they are also fingerprinted upon arrival at the US border under the US VISIT scheme. On the other hand, problems encountered in the implementation of tougher border controls at the US-Canadian border, especially the lengthening of delays at border checkpoints, led to discussions on the establishment of a new approach to border control, dubbed 'smart borders'. This approach, which foresaw the redeployment of US border controls in partner countries by means of exchanges of information and of border control personnel, was enacted through the adoption of an Action Plan for Creating a Secure and Smart Border, announced in December 2001 and endorsed in the 2002 US National Homeland Security Strategy.[3] Interestingly, the efforts associated with the establishment of such a 'North American perimeter' took their cue from EU cooperation in the context of Schengen.[4]

The European Union has experienced a similar acceleration, with initiatives that had been stopped or postponed prior to 2001 being fast-tracked (and even more so after the attacks of 11 March 2004 in Madrid).[5] **It has however initially taken a slightly different path to border control and resisted the temptation of a blanket collection of travellers' data**. It first developed the EU Visa Information System (VIS), which requires all foreign entrants subject to visa requirements to provide fingerprints and biographical details as part of the application process. Schengen consulates across the world are now being connected to the VIS and equipped to register visa applicants and process their fingerprints. VIS data are stored centrally, alongside but separately from the Schengen Information System (SIS/SIS II), which contains information about persons to be refused entry or subject to specific checks and actions. The 'smart borders' initiative builds on discussions on the feasibility and desirability of the VIS in 2004. The Entry/Exit System (EES), which forms the cornerstone of the current initiative, was then discarded as a costlier option, only to be re-introduced as a necessary complement to the VIS in the Commission's 2008 'border package' – despite the fact that the VIS had not been rolled out at the time. In lieu of a complement, however, EU 'smart borders' appear to bring the EU closer to the position held by the previous US administration on the question.

The three issues mentioned above – reversibility, necessity and originality – are thus central to the discussion of EU 'smart borders' in the context of current and forthcoming proposals on EU JHA databases. In this regard, it seems important to ask whether 'smart borders' are actually

---

[2] For further discussion, see: Hobbing, P. and Kowslowski, R. (2009), *The tools called to support the 'delivery' of freedom, security and justice: a comparison of border security systems in the EU and in the US*, PE 410.681, Brussels, February 2009.

[3] For further details see Kowslowski, R. (2005), "Smart Borders, Virtual Borders or No Borders: Homeland Security Choices for the United States and Canada", *Law & Bus. Rev. Am.*, 2005, 11(527).

[4] *Idem*. For a comparative EU-North America effort, see the outcome of the research funded by the European Commission's DG Relex on EU-Canada relations in: Scherrer, Guittet and Bigo (eds.) (2009), *Mobilités sous surveillance: Perspectives croisées UE-Canada*, Montreal: Athena, 2009; M. Salter (ed.), *Mapping Transatlantic Security Relations: The EU, Canada and the War on Terror*, London: Routledge, 2010. See also Fortmann, Roussel and Macleod (eds.) (2003), *Vers des périmètres de sécurité?: La gestion des espaces continentaux en Amérique du Nord et en Europe*, Montreal: Athena, 2003.

[5] See: Mitsilegas, V. (2005), "Contrôle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme", *Cultures & Conflits*, 2005, n°58, pp. 155-181.

about what happens at the external, territorial borders of the Member States of the EU. **The EES and the RTP are mostly about what happens before and after the border.** In conjunction with the VIS and the Schengen Information (SIS, and its would-be successor SIS II), they foresee **the establishment of pre- and post-border screening procedures targeting all foreign visitors to the EU. Associated with other data and information systems, they destabilise the foreigner/citizen divide and lay down the conditions for the proactive monitoring and statistical surveillance of a large number of persons**.

1.2 JHA databases and smart borders: The question of impact

The pace at which the EU's JHA database landscape is expanding has caused a number of tensions among EU institutions and bodies in recent years. These tensions have often been framed in reference to the right to data protection and privacy, due to the active involvement of data protection authorities, especially the European Data Protection Supervisor (EDPS) and the Article 29 Working Group on Data Protection.

Should the impact of smart borders, associated with other initiatives on 'JHA databases', be understood, however, only in terms of data protection? These tensions are certainly a reminder that matters related to 'JHA databases' might be technical, but that the questions they raise touch upon key legal and political issues. In this sense, the legal challenge related to the right to data protection cannot be overlooked. **This legal challenge is mainly embodied in the necessity debate surrounding the establishment of JHA databases, which lies at the heart of the proportionality principle test.** Observing the requirements following from the right to data protection is prerequisite, but should not be regarded as sufficient for justifying new large-scale information-exchange schemes. The monitoring and sorting of large numbers of persons, of which smart borders initiative, however, is only one component, bears the potential for significant social harm. A particular question of concern in this respect is non-discrimination, and the way in which the growing landscape of EU data and information exchange schemes **can generate effects of statistical discrimination due to the logics of profiling and data-mining pertaining to JHA databases and smart borders**.

To examine the question of impact in relation to the discussion on reversibility, necessity and originality, the study unfolds as follows:

- Section 2 examines the landscape of JHA databases in the European Union.
- Section 3 examines in detail the 'smart borders' initiative.
- Section 4 addresses the legal challenges raised by EU activities related to JHA databases, including the systems foreseen by the 'smart borders' initiative.
- Section 5 lays out recommendations for consideration by the European Parliament's LIBE (Civil Liberties, Justice and Home Affairs) Committee.

2. The Landscape of JHA Databases in the EU

KEY FINDINGS

- There is no clear or commonly shared definition of a 'JHA database'.
- Existing knowledge of JHA data and information-exchange schemes highlights the absence of a regular effort at consolidating a detailed picture of all data and information exchange in the Area of Freedom, Security and Justice, across measures and policy domains.
- The distinction between centralised and de-centralised systems among JHA databases is misleading. The EU JHA database landscape involves distributed systems, which does not mean that there is a structural guarantee that data and information exchanges are compartmentalised, and thus cannot be said to be data protection-compliant by default.
- Among these distributed systems, the distinction between personal and non-personal data is increasingly replaced by the distinction between personal and operational data, the latter involving 'anonymised' or 'depersonalised' data. The maintenance of this distinction depends on the capacity of law-enforcement agencies to effectively depersonalise data, which raises issues related to the right to data protection and more generally to the fundamentals of privacy and non-discrimination.
- The main trend in the EU landscape of JHA databases is towards multi-purpose data and information schemes, in the context of a growing convergence towards law-enforcement as intelligence rather than criminal investigation. This trend is nurtured by the focus on 'information management', understood as the promotion of information-sharing by default, availability and interoperability.
- In this context, EU agencies and bodies have increasingly become data processors in their own right, and are confronted with the implications of the above-mentioned trends. Activities linked to the management of large-scale IT systems should also be addressed in this regard, insofar as management seems to include the monitoring of research and the steering of pilot schemes to develop further JHA databases.
- Current and forthcoming proposals, especially the EU PNR and EU TFTS initiatives, raise the questions of mass data processing for law-enforcement purposes, of automated data processing and of profiling as potential future trends with regard to JHA databases.

This section examines the landscape of JHA databases in the EU, taking into account functioning schemes, current and forthcoming legislative and policy proposals. It does not detail all existing information exchange schemes related to the EU's JHA policies: a more systematic overview is provided in the analytical table on JHA Databases found in Annex 1 of this study.[6] **The aim is rather to tease out what holds this landscape together**. Are there **any commonalities** between JHA-related data and information exchange schemes, despite the

[6] A partial overview is also available in earlier work conducted on behalf of the LIBE Committee of the European Parliament, see Bigo, Carrera et al. (2011), *Towards A New EU Legal Framework for Data Protection and Privacy*, PE 453.216, Brussels, September 2011, esp. pp. 40-56; Scherrer, Jeandesboz,, Guittet (2011), *Developing an EU Internal Security Strategy, fighting terrorism and organised crime*, PE 462.423, Brussels, November 2011, esp. pp. 91-108.

differences in aims and objectives, policy domains and technical architecture? **Which kind of policy orientation do these commonalities suggest?** What is, finally, **the involvement of EU agencies and bodies in this landscape?**

The section falls into three specific parts:

- We first discuss, on the basis of currently available knowledge, whether it is possible to identify clearly what a JHA database is (2.1);
- We then proceed to examine current and forthcoming proposals (2.2) and
- We further discuss the policy orientations that common traits of JHA databases denote, including the implications of these orientations for the activities of EU agencies and bodies (2.3).

2.1 What is a JHA database?

There is no clear definition of a 'JHA database'. In the 2010 Communication where it seeks to provide an overview of such measures, the European Commission refers to 'information management', partly it seems because 'JHA databases' comprise a variety of set-ups with different purposes, technical architectures, rules of access and data protection provisions.[7] For this reason, rather than starting from a working definition, this section first examines the knowledge available to EU bodies on 'JHA databases' (2.1.1). We further discuss the key distinctions made by the Commission to categorise these schemes, and especially the three that appear central:

1. **Architecture of the scheme.** The Commission distinguishes between centralised and decentralised schemes. It further extends this discussion to point out that overall, the landscape of JHA databases is made up of distributed schemes, suggesting this is a favourable outcome for the persons concerned with these schemes. Here the question raised is whether such a distinction is meaningful when considering the impact of these schemes (2.1.2).
2. **Personal and non-personal data.** The Communication excludes from its scope measures involving "the exchange of non-personal data for strategic purposes, such as general risk analyses or threat assessments". Again, the question we raise is whether this distinction is meaningful and whether, as the Communication apparently assumes, the exchange of "non-personal data" is any less problematic than the exchange of "personal data" (2.1.3).
3. **Purpose.** The Communication establishes for each scheme the 'main purpose' that it is related to. The very formulation used in the document does suggest that one of the characteristic trends of the current landscape of JHA data and information exchange schemes is the move towards multi-purpose measures, which are attributed a 'main' or preferential purpose but generally serve others as well (2.1.4).

For each of the points addressed below, we will point out issues that will be explored further in the remainder of the study, and outline a set of questions which can be raised by the LIBE Committee in future discussions on JHA databases.

[7] European Commission (2010), *Overview of information management in the area of freedom, security and justice*, COM(2011) 385 final, Brussels, 20.7.2010.

2.1.1 JHA databases: What is the available knowledge?

How much knowledge do EU agencies and bodies have of exchanges of information related to JHA policies? Such a question is not purely rhetorical given the expansion of this policy domain as well as the multiplication of initiatives in the area of information exchange since the beginning of the 2000s. We will return to this discussion, but the fact that it is only in November 2009 that the Council adopted a EU information management strategy (IMS) suggests in addition that this process has advanced in mostly *ad hoc* terms – hence the question of available knowledge.

The first overview of these issues is the above-mentioned Commission Communication of July 2010 on "information management in the area of freedom, security and justice". The need for such an overview is framed in three different ways in the document:[8]

1. As a way to inform citizens of "what personal data are processed and exchanged about them, by whom and for what purpose";
2. As a contribution to an "informed policy dialogue with all stakeholders" and
3. As a response to "calls by Member States to develop a more 'coherent' approach to the exchange of personal information for law enforcement purposes", in the context of the adoption of the EU Information Management Strategy and of the objective laid down in the Stockholm Programme of developing a "European Information Exchange Model".

What surfaces through these three points is certainly the difficulty for practitioners themselves to keep track of precisely which kind of information is exchanged, and by which means – let alone for citizens and civil society groups. This raises two issues:

1. On the quality and indeed possibility of reporting on data and information schemes in EU JHA policies for the information of EU institutions, concerned citizens, groups and organisations and the general public. The contents of the Communication highlight the piecemeal character of information related to the actual use of JHA information-exchange schemes. The effort put into the statistical annex of the document is welcome, but also **points out the absence of a regular (possibly yearly) effort at consolidating an overall picture of information exchange in the field of justice and home affairs**. Such reporting is available for a number of schemes, e.g. the SIS for border control,[9] Eurodac for the EU asylum policy[10] or the Prüm decision and for police cooperation.[11] For other set-ups such as the 'Swedish initiative', some data are available but not on a regular basis.[12]

---

[8] *Ibid*, p. 3.

[9] Circulated by the Council Secretariat on a yearly basis. For the latest (2011) SIS statistics, see: Council of the European Union (2012), *Schengen information system database statistics 01/01/2012*, 8281/12, Brussels, 28.3.2012.

[10] Circulated by the European Commission to the Council and the European Parliament. For the latest instalment, see: European Commission (2012), *Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit in 2011*, COM(2012) 533 final, 21.9.2012.

[11] Circulated by the Council General Secretariat to the Working Party on Data Protection and Information Exchange on a yearly basis. For the latest instalment, see: Council of the European Union (2012), *Statistics and reports on automated data exchange for 2011*, 11367/12, Brussels, 20.6.2012.

[12] In May 2011, the Commission forwarded to the Council a report on the operation of the "Swedish initiative" on the basis of Article 11 of Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L386/89, 29.12.2006). See: European Commission (2011), *Operation of the Council*

2. On the effective handling of data and information: is it possible for the agencies, bodies and services involved in the daily handling of data and information to keep track of what is available, where and how, and how this affects their own input? This question involves important issues such as **the possibility of multiple entries, data and information duplication, overlaps and quality of data and information**. Another issue is the **competition between practitioners in access to data and information-exchange schemes and control over them**: such competitions can go some way to explain the current proliferation of 'JHA databases' and further increase the risks of multiple entries, duplication, overlaps and poor quality of data.

The second overview of information exchanges related to EU JHA policies produced in recent years has taken place in the context of the Union's border control policy, following the so-called '29 measures' Council Conclusions of 1 March 2010.[13] Under the aegis of the Belgian federal police, Project Group 'Measure 6' set out to build "an accurate picture of the actual situation of the information gathered and/or processed within the MS and […] EU agencies and bodies on illegal immigration, illegal immigration networks, and trafficking of human beings and as a longer term objective other forms of cross border crime covered by integrated border management".[14] The final report of the project includes descriptive flowcharts between stakeholders.[15] The need to undertake the project in the first place further confirms the notion conveyed by the Commission's 2010 Communication that **the practitioners involved either in policy decisions about exchanges of information or in their actual conduct have a sometimes-limited overview of their breadth and depth**. A further question is the extent to which the strategic vision articulated by documents such as this communication or the European Information Management Strategy (discussed below in 2.3.1) is actually shared by practitioners beyond the specific groups in charge of strategy and policy development.[16]

The European Commission's DG Home is currently undertaking the third overview effort as part of the European Information Exchange Model (EIXM) project. EIXM will be presented in a Commission Communication expected in December 2012. EIXM is steered by Directorate A (Internal Security) as part of the police and justice cooperation aspects of the EU's JHA policies. This leads to a question regarding the limited overview that practitioners have of data and information exchange: **To what extent is it due to diverging priorities, if not outright tensions, among various agencies, bodies and services?** Each scheme reviewed in this study services and is steered by specific groups of practitioners. In the case of the European Commission's DG Home, Directorate A is involved with schemes such as the Prüm Decision or the Swedish initiative (although the extent of the Commission's competencies are limited), while Eurodac, SIS II and VIS are steered by several units in Directorate B and Directorate C, in most cases with distinctions between 'policy' units and 'technical' units (Eurodac being the only exception, the policy and technical teams being regrouped in Unit Home B.2). The question of the depth and breadth of intra- and inter-service consultations for the purpose of the EIXM will therefore be central when assessing the results of the Commission's review exercise.

Framework Decision 2006/960/JHA of 18 December 2006 ("Swedish Initiative"), SEC(2011) 593 final, Brussels, 13.5.2011.

[13] Council of the EU (2010), *Council Conclusions on 29 measures for reinforcing the protection of the external borders and combating illegal immigration*, 6975/10, Brussels, 1.3.2010.

[14] Council of the EU (2010), *Project Group on measure 6*, 14011/10, Brussels, 24.9.2010, p. 2.

[15] Council of the EU (2011), Final report and recommendations of Project Group "Measure 6", doc. 7942/2/11, Brussels, 6 July 2011, pp. 14-21.

[16] For a discussion, see Scherrer, Jeandesboz and Guittet (2011), *Developing an EU Internal Security Strategy*, op. cit., esp. Ch 1.2.

The two completed overview exercises so far and EIXM in name have two points in common:

1. They suggest, firstly, that decision-makers and practitioners involved with exchanges of information **have a limited grasp of the overall picture of information exchange related to the EU's JHA policies**. This limited grasp should be understood in relation with the tensions between the various groups involved with each specific scheme. **This further raises the question of the capacity of concerned citizens, groups and organisations outside relevant institutions and bodies to obtain satisfactory information on the use of personal data and information exchange**, outside of fairly circumscribed policy areas and information exchange schemes.
2. They do not allow identifying the main characteristics of what would be an EU 'JHA database'. In the 2010 Commission Communication, 'information management' is not a clear terminology, and encompasses schemes with different technical architectures and purposes. The only exclusion criteria is that exchanges of information involving so-called 'non-personal data', i.e. operational and strategic information, fall outside the scope of the overview. This appears to be an uneasy distinction: some information exchange schemes, such as the Analytical Work Files (AWFs) component of the Europol information system (EIS) combine both operational information and personal data (EIS features in the 2010 Communication in this regard). Furthermore, the notion that 'non-personal data' are less problematic has to be examined further: while 'non-personal data' fall outside the scope of data protection concerns, their use might still generate social harm and result in discriminatory effects.

2.1.2 A distributed layout of data and information exchange schemes

The 2010 "overview of information management" Communication from the European Commission distinguishes between two categories of schemes related to the exchange of information in the context of the EU's justice and home affairs policies: centralised and decentralised. Schemes with a centralised architecture – i.e. which literally comprise a 'central unit' include for instance Eurodac, the SIS and the VIS. Decentralised set-ups are exemplified by the Prüm Decision scheme or the 'Swedish initiative' scheme.

Although this configuration is the result of EU JHA data and information schemes having been developed in an *ad hoc* manner, **the argument has emerged that it was in fact a *de facto*, technical limit to data processing**. The point is repeatedly stressed in the 2010 Communication, which argues that: "A single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing […] [S]uch a system would, however, constitute a gross and illegitimate restriction of individuals' right to privacy and data protection and pose huge challenges in terms of development and operation […] The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' right to privacy than any centralised alternative".[17]

This assessment of EU JHA exchanges of data and information schemes should however be considered thoroughly. **The notion of a fully centralised, multi-purpose and stand-alone EU JHA database against which it stands is firstly theoretical at best**. Obstacles to such a development include issues pertaining to the right to data protection and the right to privacy indeed, but also such key principles governing the competencies of the Union as the principle of subsidiarity and proportionality (Art. 5 TEU). One could also argue that **this idea would encroach upon the principle of internal security being an exclusive competence of the Member States (Art. 72 TFEU) and would also affect the balancing of (shared)**

[17] COM(2010) 385 final, *op. cit.*, p. 3.

competences outlined in Art. 4.2. TFEU. Secondly, **the contrast between centralised and de-centralised**, and the assumption that a de-centralised layout supports the strict compartmentalisation of data, **can be misleading**. Given the priorities governing the layout of data and information exchange schemes in EU JHA policies, chiefly availability and interoperability (see point 2.3.2 below), **it is more accurate to think of them as distributed schemes, involving not only a closer association of operational and personal data, but also a trend towards multi-purpose processing of data**.

2.1.3 A closer association of operational and personal data

As mentioned previously, the distinction between the exchange of personal data and 'non-personal data' is the key exclusion criteria adopted by the European Commission in its 2010 Communication to define 'information management in the EU'. The assumption is that JHA-related information exchange is divided in two 'streams':

- Exchange of operational and strategic information, which should as a principle not include personal data, and
- Exchange of personal data.

This distinction, however, is not always useful to understand current trends in the JHA database landscape, insofar as **a growing emphasis is placed on the use of personal data as part of operational and strategic cooperation** between national authorities and EU bodies. In addition, it is important to point out that **the distinction between operational and personal chiefly depends on the capacity of law-enforcement actors to personalise or 'anonymise'/'depersonalise' data**. Two examples of this trend can be discussed for illustration purposes.

Europol AWFs (analytical work files): AWFs are used in the context of Europol for analysis purposes, defined as "the assembly, processing or use of data with the aim of assisting criminal investigations, in accordance with Article 14(2) of the Europol Decision".[18] Analysis tasks can be of a strategic type, or related to a specific case, and AWFs are created on the basis of an 'opening order'.[19] While there are clear rules establishing the specificity of personal data and its handling in the context of analysis, the tasks entrusted to Europol entail the use of personal data for strategic and/or operational purposes.

Frontex Information System (FIS): while foreseen in the original Frontex regulation,[20] the extent to which the FIS has been implemented to this day and what it consists of remain unclear. It can be assumed that it will, or does constitute a platform and secure communications network with different modules, similar in outlook if not in functionalities to the EIS. At least one of these modules is referred to by Frontex staff as ANTOOLS, a computer programme handling various categories of data for the purpose of analysis.[21] The legal basis for the FIS has been modified significantly with the adoption of the amended Frontex Regulation in 2011 (hereafter Frontex Regulation), introducing explicit references to EU agencies and specifying that Frontex "shall develop and operate an information system capable of exchanging classified information"

---

[18] Council of the EU (2009), Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, OJ L 325/14, 11.12.2009 (hereafter "AWF rules"), Art. 1(c).

[19] See respectively AWF Rules, Art. 11, and Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ L 121/37, 15.5.2009 (hereafter "Europol Decision"), Art. 16.

[20] Council of the EU (2007), Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Coordination at the External Borders of the Member States of the European Union, OJ L 349/1, 25.11.2004 (hereafter "Frontex Regulation"), Art.11.

[21] Frontex (2010), *Beyond the Frontiers*, Warsaw, 2010, p. 67.

with the actors specified in Art. 11 and Art. 13.[22] The amended Frontex Regulation introduces the possibility for the agency to process personal data collected during joint operations, pilot projects and rapid interventions that has either been collected by Frontex officials or transmitted by Member State authorities in this context.[23] "Further processing", that is, the use of this personal data beyond its collection, involves the transmission to Europol and "other Union law enforcement agencies" on a case-by-case basis and the preparation of risk analyses (in which case "data shall be depersonalised".[24] Again, personal data here will be processed for strategic and/or operational purposes, an issue that will be further enhanced with the establishment of EUROSUR (discussed in point 3.3.2 below).

The distinction between the exchange of personal data and 'non-personal data' raises obvious legal challenges from the point of view of data protection and privacy that will be further addressed in point 4.1.2. 'Depersonalisation' does not mean that the exchange of data and information cannot create social harm, furthermore, especially in relation to the question of non-discrimination (see further 4.2).

2.1.4 The trend towards multi-purpose data and information exchange schemes

Is it possible to define JHA databases in terms of their relation to a specific JHA purpose? There is undeniably a link between specific data and information exchange schemes and policy areas, e.g. Eurodac for the implementation of the EU's asylum policy or VIS for the EU's visa policy. In the meantime, **this link is preferential, not exclusive**. As explored in the analytical table in Annex 1, a number of JHA data and information schemes in the EU have seen their purpose evolve, or constitute multi-purpose measures in their own terms. There are several cases to consider in this respect.

Firstly, attempts have been made **to expand the purposes of an existing instrument** through legislation. The recurrent debates over access by law-enforcement to Eurodac are a good example. Eurodac was initially established for the comparison of fingerprints for the purpose of implementing the Dublin Convention.[25] Since then, the Council, European Council and European Commission have addressed the access to Eurodac by law-enforcement agencies on several occasions.[26] The European Commission has proposed to introduce such possibility in its 2009 amended recast proposal for the Eurodac Regulation. The proposal sought to introduce a 'bridging clause' to "allow consultation of Eurodac by law enforcement authorities for the purpose of prevention, detection and investigation of terrorist offences and other serious

---

[22] Council of the EU (2011), Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Coordination at the External Borders of the Member States of the European Union, OJ L 304/1, 22.11.2011.

[23] Frontex Regulation, Art. 11c.

[24] Frontex Regulation, Art. 11(3).

[25] Council of the EU (2000), Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316/1, 15.12.2000 (hereafter "Eurodac Regulation").

[26] Among others, in the 2004 Hague programme for the area of freedom, security and justice and the 2005 communication from the Commission on interoperability and synergies among JHA databases, see: Council of the European Union (2004), *The Hague Programme: strengthening freedom, security and justice in the European Union*, 16054/04, Brussels, 13.12.2004; European Commission (2005), *Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597 final, Brussels, 24.11.2005.

criminal offences".[27] The proposal received critical attention from the European Data Protection Supervisor (EDPS) on account of its timing, of its necessity given the already available possibilities for law-enforcement authorities to have access to fingerprint data, and of the impact it might have on an already-vulnerable group.[28] While it withdrew the provisions regarding law-enforcement access in its following 2010 recast proposal, the European Commission has recently returned to this idea, with yet another recast version of the Eurodac Regulation.[29] The proposal has been met with an equally critical opinion from the EDPS.[30]

Secondly, **we have seen the case where new purposes have been added to a data and information exchange scheme while it was already under development but not operational**. For the moment, this specifically concerns the second-generation SIS and VIS. In its 2010 overview of information management communication, the European Commission indicates, "while most of the instruments […] analysed have a unitary purpose […] SIS, SIS II and VIS appear to be the main exception to this pattern".[31] This is in part due to the decision-making process involved in the establishment of SIS II and VIS. Measures related to the technical implementation of the schemes were adopted before legislative instruments established their scope and purpose (Regulation 2001/2424 and Council Decision 2001/886 for SIS II, Council Decision 2004/512/EC for VIS), mostly due to political disagreements over how these systems

---

[27] European Commission (2009), *Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, COM(2009) 342 final, Brussels, 10.9.2009.

[28] EDPS (2010), *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/...) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (2010/C 92/01)*, OJ C 92/1, 10.4.2010.

[29] See, respectively, European Commission (2010), *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)*, COM(2010) 555 final, Brussels, 11.10.2010; European Commission (2012), *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)*, COM(2012) 254 final, Brussels, 30.5.2012.

[30] EDPS (2012), *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/...] [.....] (Recast version)*, Brussels, 5.9.2012.

[31] European Commission (2010), *Overview of information management*, op. cit., p. 22.

should be used. In this configuration, SIS II has notoriously been developed as a 'flexible tool' and the SIS II Regulation[32] leaves a significant margin of interpretation regarding:

1. the purpose of the system, which is "to ensure a high level of security within the area of freedom, security and justice" with mentions of "public security", "public policy", "the safeguarding of security in the territories of the Member States" as well as "to apply the provisions of Title IV of Part Three of the Treaty" (Art.1.2).
2. access to the system: access to SIS II is in general enabled through N.SIS II Offices established by each Member State (Art. 7). Art. 27 further establishes the list of authorities with access to SIS II alerts (access to data and right to search) but has been presented as introducing a degree of ambiguity by referring to the right of access by "coordinating authorities", without identifying them further.[33]

In the case of VIS, the VIS Regulation introduced four years after the decision to proceed with the technical development of the system was adopted, establishes that the VIS should also be used as a measure to facilitate the fight against fraud and irregular stay in the territory of the Member States (Art. 2).[34] It is 'complemented' by Council Decision 2008/633/JHA which creates the possibility for Member States' 'designated authorities' and for EUROPOL to access VIS for the purpose of "prevention, detection and investigation of terrorist offences and other serious criminal offences" (Art.1).[35]

The tensions generated over this question among EU bodies should not be underestimated: in the case of SIS II, for instance, the European Parliament has repeatedly opposed the 'flexibility option'.[36] This trend, among others, brings about legal challenges concerning (un)purpose limitation, and generates concerns about the effects of statistical discrimination arising from multi-purpose databases (see further 4.1.5, 4.2.2 below). **The development of SIS II and VIS also establishes a problematic precedent with regard to forthcoming proposals involving the development of new data and information-exchange schemes**. The issue concerns both current proposals for the establishment of an EU Passenger Name Record system and an EU Terrorist Finance Tracking System (see 2.1.5) and the upcoming legislative proposal on 'smart borders' (see Section 3 below).

---

[32] European Parliament and Council of the EU (2006), Regulation (EC) No 1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4, 28.12.2006.

[33] See the comments by the EDPS on the proposal for the SIS II regulation: EDPS (2006), *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final),* OJ C 91, 19.4.2006.

[34] European Parliament and Council of the EU (2008), Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218/60, 13.8.2008.

[35] Council of the EU (2008), Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218/129, 13.8.2008.

[36] See further Bigo, Carrera et al. (2011), *Towards A New EU Legal Framework for Data Protection and Privacy*, op. cit., Chp. 3.

2.1.5 Current and forthcoming proposals: EU PNR and EU TFTS

Two key proposals are currently forthcoming or under discussion which, should they be adopted, would further expand and arguably accelerate the transformation of the EU landscape of JHA and information exchange schemes: the proposal for EU PNR and EU TFTS. To recapitulate briefly:

1. **EU PNR**: The European Commission initially tabled a proposal for the establishment of an EU PNR in November 2007. With work under way in the Council from February 2008 onwards, the European Parliament refused in November 2008 to vote on the issue. The European Commission tabled a new proposal in February 2011, together with an impact assessment document.[37]

2. **EU TFTS:** The idea of establishing an EU equivalent to the US Terrorist Finance Tracking Programme (TFTP) was initially proposed by the European Parliament. The aim was to prevent bulk data transfers from the financial services company SWIFT to the US authorities in the context of TFTP and ensure that extraction and analysis of SWIFT data would take place within the jurisdictions of the EU and its Member States. In July 2011, the European Commission tabled a Communication considering the 'available options' for the EU TFTS.[38] A legislative roadmap was filled the same month by DG Home, announcing that a legislative proposal was to be expected in the first quarter of 2012, but this has yet to materialise.[39]

The questions discussed throughout this note apply to these proposals. Both EU PNR and EU TFTS have been discussed for some years now and have stirred significant political controversies, which do raise the question of **whether the policy orientations embodied in these initiatives should not be reversed**. The **assessment of their necessity also varies significantly**, as illustrated by the positions adopted by the European Parliament on EU-PNR: while extremely critical about the 2007-08 iteration of the proposal, the draft report submitted to the LIBE Committee in February 2012 endorses the Commission's view with only minor modifications.[40] Finally, **both proposals demonstrate the importance of the question of originality, as they both derive from measures implemented by the US administration and other third countries** (in the case of PNR, Australia in particular) and their effects on EU policies. The relevance of originality is highlighted by the reference introduced in the Commission Communication on EU TFTS that "a European equivalent system [to the TFTP] would not necessarily have to copy all elements of the US TFTP […] an EU system should be set up taking into consideration the specificity of the EU legal and administrative framework into consideration, including the respect of applicable fundamental rights".[41]

---

[37] European Commission (2011), *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, 2.2.2011, Brussels and accompanying documents SEC(2011) 132 and SEC(2011) 133 final

[38] European Commission (2011), *A European terrorist finance tracking system: available options*, COM(2011) 429 final, Brussels, 13.7.2011.

[39] European Commission (2011), *Legislative proposal establishing a legal and technical framework for a European Terrorist Finance Tracking System (EU TFTS)*, Bussels, July 2011.

[40] European Parliament (2011), *Draft report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 – C7-0039/2011 – 2011/0023(COD)) - Committee on Civil Liberties, Justice and Home Affairs*, 2011/0023(COD), Brussels, 14.2.2012.

[41] COM(2011) 429 final, op. cit., p. 4.

These proposals further echo the specific issues raised with regard to the EU landscape of JHA data and information-exchange schemes. **The trend towards multi-purpose is reaffirmed in the case of EU PNR**, for instance, whose scope includes, according to the current legislative proposal from the Commission, the "prevention, detection, investigation and prosecution" of both terrorist offences and serious organised crime (Art. 1.2). **The ambiguities associated with the development of SIS II and VIS are also of potential concern**: the latest discussions among Member States' representatives over the future Internal Security Fund currently lean towards the inclusion of provisions regarding the funding of these two systems in the related legislative instrument, regardless of the prospect of an agreement over the scope and aims of such schemes. Art. 4(1)(e) of the revised compromise proposal by the Presidency thus specifies at this stage that the instrument would support costs associated with the development of EU PNR, while some Member States' representatives have expressed a preference for retaining references to the EU TFTS.[42]

These two proposals – current and possibly forthcoming – also point out upcoming trends within the EU JHA database landscape. **The various iterations of the EU PNR proposal have attracted significant attention due to the change of scale in data processing**: the system would have to handle **an estimated 500 million personal records** according to the Commission's impact assessment,[43] against an average of less than 1 million personal records over the past 10 years for the SIS, or 70 million in any given period of five years for the VIS once it is fully deployed.[44] The EU PNR proposal is further notable for **its introduction of 'automated processing'** for purposes of assessment in real time or pro-actively of the degree of risk presented by passengers – **in other words, profiling**.[45] As the density of data and information exchange involved in EU JHA policies increases, the possibility and indeed desirability of such automated processing for purposes of assessment can potentially become increasingly central. It is important **to keep in mind the possible social harm that such orientations can bring about**, in the context of the right to data protection but more broadly with regard to privacy and non-discrimination (a point further developed in section 4.2 below).

As we further discuss in the next pages, finally, **these proposals also fit within the move towards multi-purpose intelligence schemes**, which constitute the key trend in the current development of the EU JHA database landscape.

2.2 The convergence towards law-enforcement as intelligence work

The study has examined so far the trends characterising JHA-related data and information exchange schemes and current as well as forthcoming proposals. In the following pages, we examine the point of convergence of these trends, namely what a number of policy and scholarly studies have qualified as a move towards JHA databases as generalist intelligence tools.[46] This convergence towards intelligence is sustained by the characterisation of a European

---

[42] Council of the EU (2012), *Draft Regulation of the European Parliament of the Council establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management - Revised compromise proposal by the Presidency*, 14357/12, Brussels, 2.10.2012, pp. 17-19.

[43] SEC(2011) 132, *op. cit.*, p. 31.

[44] Scherrer et al. (2011), *Devising an EU Internal Security Strategy*, op. cit., pp. 102-103.

[45] See e.g. De Hert, Bellanova (2009), *Data Protection in the Area of Freedom, Security and Justice: A System to Be Fully Developed?*, PE 410.692, March 2009.

[46] See e.g. Brouwer, Evelien (2008), *Digital Borders and Real Rights*, Leiden: Martijnus Nijhoff Publishers, 2008; Scherrer et al. (2011), *Devising an EU Internal Security Strategy*, op. cit.; Hobbing, P., Koslowski, R. (2009), *The tools called to support the 'delivery' of freedom, security and justice: a comparison of border security in the EU and the US*, PE 410.681, Brussels, February 2009; Wills, Vermeulen et al. (2011),

internal security model defined in terms of pro-active and intelligence-led policing (2.2.1) and by the shaping of an 'information exchange by default' option in the management of data and information exchange (2.2.2). We further outline the role of EU bodies in this configuration, with a specific focus on the two core 'JHA agencies', Europol and Frontex, as well as the upcoming EU agency for large-scale IT systems (2.2.3).

2.2.1 The European internal security model: Pro-active and intelligence-led policing

Despite the variety of measures considered as 'JHA databases', existing as well current and forthcoming systems are framed as a contribution to a model of EU internal security premised on pre-emptive and intelligence-led policing.

References to proactivity and intelligence in EU JHA policies are not new. Recent developments have however brought these references to the forefront of the debate. Although a symbolic contribution more than an effective policy document, the 2010 European Internal Security Strategy (ISS) thus embraces an outlook of "prevention and anticipation, which is based on a proactive and intelligence-led approach".[47] In a similar but more hands-on perspective, the idea of a 'policy cycle' in EU internal security, which was developed through the Harmony project,[48] places intelligence and its use through strategic analysis tasks (consolidated in Europol OCTA and SOCTA reports) at the heart of EU home affairs policy planning.[49] This has also implications in operational terms. The so-called 'Swedish initiative' is an instructive example; particularly in the way the legal instrument that establishes this data and information exchange scheme distinguishes between the notions of 'criminal investigation' and 'criminal intelligence operation'.[50] According to Framework Decision 2006/960/JHA, a criminal investigation is "a procedural stage within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts" (Art. 2(b)). A criminal intelligence operation, on the other hand, is "a procedural stage, not yet having reached the stage of a criminal investigation, within which a competent law enforcement authority is entitled by national law to collect, process and analyse information about a crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future" (Art. 2(c)). The inclusion of 'criminal intelligence operation' considerably widens the scope of data and information exchange, as well as the purpose of this exchange: **Given that 'criminal intelligence operations' are concerned with crimes that may be committed, there is potentially no time limitation to the processing of data in such circumstances**.

Access to personal data as much as operational and strategic information (with the above-mentioned limits to such a distinction) is central in a model based on pro-active and

---

Parliamentary oversight of security and intelligence agencies in the European Union, PE 453.207, Brussels, June 2011;

[47] Council of the EU (2010), *Draft Internal Security Strategy for the European Union: "Towards a European Security Model"*, 5842/2/10, Brussels, 23.2.2010, p. 11.

[48] Council of the EU (2010), *Result of the "Harmony" project - "A generic European Crime Intelligence Model - Bringing together the existing instruments and strengthening Europol's central role*, 14851/10, Brussels, 25.10.2010.

[49] See Scherrer et al., *Developing an EU Internal Security Strategy*, op. cit., esp. pp. 42-45.

[50] Council of the EU (2006), Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union, OJ L386/89, 29.12.2006.

intelligence-led policing. As argued in the ISS, "[i]f law-enforcement authorities are to be able to prevent and act early, they must have timely access to as much data as possible concerning criminal acts and their perpetrators, modus operandi, details of victim(s), vehicles used, etc".[51] These prescriptions comprise two dimensions. On the one hand, they imply **an extensive view of access for law-enforcement authorities**, an idea that underpinned the possibilities of access afforded to public authorities to the VIS for example, but also Eurodac. In the Eurodac case, access to stored fingerprints of asylum seekers by law-enforcement agencies is typically justified in terms of an 'information gap' to be bridged. This also goes hand-in-hand with **a very wide understanding of what kind of data and information law-enforcement agencies should have access to**. To return to the above-mentioned example of the 'Swedish initiative', the scope of exchanges include "any type of information or data that is held by law-enforcement authorities" and "any type of information or data that is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures, in accordance with Article 1(5)".[52] On the other hand, these prescriptions **point towards the possibility of data-driven action in the field of internal security**. This is typically the case of the EU PNR proposal discussed above, where possibilities for identification afforded by access to 'traditional' information systems such as SIS II or VIS for instance, would be expanded by means of profiling measures in order to detect 'unknown unknowns'.

2.2.2 Distributed, available and interoperable: JHA databases and 'data-sharing by default'

The idea of a 'proactive and intelligence-led' model for EU home affairs has been translated into a set of more specific prescriptions regarding JHA databases. The EU Information Management Strategy (IMS) for EU internal security **characterises these prescriptions as contributing to 'an attitude of data-sharing by default' among the Union's law-enforcement authorities**.[53] While it is far from being effective in practice, this position should lead to a reassessment of the notion that the JHA database landscape is compartmentalised. More precisely, ***de facto* and *de jure* compartmentalisation is mitigated by the notions that information should be available and that data and information schemes should provide for interoperability**.

Availability. The ISS explicitly aims for "[a]n internal security policy supported by information exchange on a basis of mutual trust and culminating in the principle of information availability".[54] The so-called 'principle of availability' constitutes a long-standing discussion among EU bodies. It was first formally mentioned in the 2004 Hague programme on the area of freedom, security and justice. In 2005, the European Commission's Communication on European databases in the AFSJ defined availability as entailing "that authorities responsible for internal security in one Member State or Europol officials who need information to perform their duties should obtain it from another Member State if it is accessible there".[55] Availability, however, has no legal standing. The proposal for a Council Framework Decision on the matter,

---

[51] Council of the EU (2010), Council document 5842/2/10, *op. cit.*, p. 13.

[52] Council of the EU (2006), Framework Decision 2006/960/JHA, op. cit., Art. 2(d) i. and ii.

[53] Council of the EU (2009), *Draft Council Conclusions on an Information Management Strategy for EU internal security*, 16637/09, Brussels, 25.11.2009, p. 10.

[54] Council of the EU (2010), Council document 5842/2/10, *op. cit.*, p. 13.

[55] European Commission (2005), *Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597 final, Brussels, 24.11.2005, p. 3.

tabled by the European Commission in October 2005,[56] was turned down by Member States' representatives, and the Council adopted in its stead the above-mentioned 'Swedish initiative' Framework Decision (2006/960/JHA). This instrument, however, does not confer a legal standing to the notion of availability.

Interoperability. The same reflection applies to interoperability. The European Commission defines interoperability as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge".[57] While availability aims to regulate the behaviour of Member States' law-enforcement authorities in EU, bilateral and multilateral cooperation, interoperability regulates the possible direct interconnections between information systems themselves. While mentioned on a regular basis, however, there have been very few developments in this area since the European Commission, in its 2005 Communication, indicated that it considered "it […] up to each Member State to analyse how national systems could better interact".[58] It is worth pointing out, however, that two EU databases, the VIS and the SIS II when it will be implemented, share the same communication system (the European Commission's s-TESTA) and the same handling system for biometrics (the Biometric Matching System, specifically tailored for them). As recalled elsewhere, furthermore, work has been conducted to develop a European-wide Universal Messaging Format in the context of the Swedish initiative and the Prüm decision, as well as on informational architectures capable of delivering services irrespective of the platforms they are based on (so-called 'service-oriented architectures' or SOA).[59]

Information management. Discussions of interoperability and availability, as suggested previously, have in the last few years been reframed as 'information management'. The term surfaced in the 2008 "Future of European Home Affairs" report and became of official use in the 2009 eponymous strategy.[60] Information management is a protean notion encompassing availability, interoperability as well as the idea that information exchange is the default position in the EU JHA database landscape. In the words of the IMS, information management is hence "functionally defined, i.e. depends on the task to be carried out, as opposed to competence-based or organisationally defined".[61] Just like availability and interoperability, then, information management is defined in terms of technical challenges rather than in legal terms. This is an issue because, just as in the case of 'criminal intelligence operations' discussed previously, there is potentially no limit, temporal or otherwise, to the activities included under the label of 'information management'.

2.2.3 JHA databases and the role of EU agencies and bodies

In the configuration examined so far, EU agencies and bodies in JHA policies exchange schemes have a key stake in obtaining access to and control of data and information. To a large extent, the current situation is the outcome of the historical reluctance of member state representatives to confer direct operational responsibilities on EU agencies and bodies (bodies here refer in particular to the units in the European Commission tasked with managing specific

---

[56] European Commission (2005), *Proposal for a Council Framework Decision on the exchange of information under the principle of availability*, COM(2005) 590 final, Brussels, 12.10.2005.

[57] European Commission (2005), COM(2005) 597 final, *op. cit.*, p. 3.

[58] *Ibid*.

[59] Bigo, Carrera et al (2011), *Towards A New EU Legal Framework for Data Protection and Privacy*, op. cit., p. 50.

[60] Future Group (2008), *Freedom, Security, Privacy - European Home Affairs in an open world*. Brussels, Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, June 2008.

[61] Council of the EU (2009), Council document 16637/09, *op. cit.*, p.

databases such as Eurodac or the VIS). This is particularly clear in the cases of Europol and Frontex, which operate as liaison and intelligence bodies rather than as an 'EU police' or 'EU border guard'.[62] In the JHA database landscape, EU agencies and bodies are currently both data processors, and database managers.

2.2.3.1 EU bodies as data processors

The terminology of data processors originates in data protection law and applies to personal data. As we have suggested previously, however, the activities of EU bodies, chiefly Europol and increasingly Frontex, **challenge the notion that there is an established distinction between personal data on the one hand, and operational/strategic data on the other** – or rather, that **personal data are increasingly considered, in the context of a pro-active and intelligence-led approach to EU home affairs, as operational and/or strategic information**.

The Europol AWFs are a clear illustration of this. The personal data that can be processed in AWFs include biographical data, physical descriptions, identification means (identity documents but also images or biometrics, including fingerprints, DNA profiles, voice profiles, blood group or dental information), occupational, economic and financial, behavioural data, as well contacts and associates, information relating to criminal activities and so forth.[63] These data can be used to provide national law-enforcement authorities with 'cross-match reports' (notification of a link between two or more items of data in two or more different national criminal cases), operational analysis reports aiming at building a picture of the activities of a specific group of persons, or strategic analysis reports that do not contain personal data as such, but for the purpose of which personal data have been processed.

Europol's data and information exchange schemes, including the AWFs, also illustrate how the work of EU bodies is affected by the dynamics of the EU JHA landscape. As the agency points out in its 2011 activity report:

- a new version of the EIS was developed to include a hit/no-hit search function to effectively widen access to the EIS beyond the national Europol National Units.
- Work is reportedly under way to enable a direct connection between the Office's Secure Information Network Application (SIENA) to national case management systems, which will establish a single gateway at national level for both national cases and cross-border cases.
- A new function has been established within Europol's data and information exchange schemes, the Europol Links Monitor, that renders various components of the schemes more interoperable by enabling automated cross-checking in certain circumstances.
- Europol has implemented, in line with its 2012 work programme and as confirmed by its 2013 work programme,[64] a 'new concept' for AWFs. In their earlier version, the AWFs consisted of 23 separate files, but the new concept will reduce this to only two files, the first one on serious and organised crime (AWF SOC), the second one on counter-terrorism (AWT CT), with the consequence of expanding the range of information

[62] See the examination of JHA agencies in Scherrer et al (2011), *Devising an EU Internal Security Strategy*, op. cit., pp. 46-86.

[63] Fully listed in Art. 6(2) of AWF rules.

[64] Council of the EU (2011), *Europol Work Programme 2012*, 13516/11, Brussels, 25.8.2011; Council of the EU (2012), *Europol Work Programme 2013*, 12667/12, Brussels, 17.7.2012.

> analysts working with the AWFs have access to (albeit with limits).[65] The maintenance of the distinction between AWF SOC and AWF CT, in this regard, is the outcome of the insistence of counter-terrorism specialists that their area of focus should remain separate from the remainder of EUROPOL activities, hinting at the dynamic identified above of appropriation of specific data and information schemes by specific professional constituencies. [66]

The examination of the Europol case would of course warrant a much more specific inquiry to do it justice.[67] It does illustrate, however, the multilayered quality of interrogations related to the development of the EU JHA database landscape, which can be applied to relations between data and information exchange schemes but also to the relations between the various components of the same information system.

Recent developments concerning Frontex hint at similar transformations. As mentioned previously (2.1.3), the revision of the agency's founding regulation has expanded its prospects with regard to data processing. **One issue of interest in view of the current EU legislative agenda will be the outcome of the negotiations over the proposal for a regulation establishing the European Border Surveillance System (EUROSUR)**.[68] EUROSUR is presented as a necessary measure "in order to strengthen the information exchange and operational cooperation between national authorities of the Member States and with Frontex".[69] In the explanatory statement of the proposal, the European Commission explains that "EUROSUR is not intended as a system to regulate the collection, storage or cross-border exchange of personal data, it was not covered by the Commission's Communication on an overview of information management in the area of freedom, security and justice of 2010".[70] **The legislative proposal however considers the possibility of processing personal data in EUROSUR, although it does so in a Recital** (No 7), whereby "[a]ny exchange of personal data using the communication network for EUROSUR should be conducted on the basis of existing national and Union legal provisions and should respect their specific data protection requirements". EU legal instruments mentioned as providing data protection requirements include the Data Protection Directive (95/46/EC), Regulation (EC) 45/2001, Council Framework Decision 2008/977/JHA and the Frontex Regulation. While a fuller analysis of the EUROSUR proposal is certainly necessary, **the main point for the purpose of this note is that considering personal data as operational data can challenge legal certainty** with regard to the applicable framework for protecting fundamental rights.

---

[65] See the commentary by members of the Europol Data Protection Officer: Drewer, Ellerman (2012), Europol's data protection framework as an asset in the fight against cybercrime, ERA Forum, Volume 13, Issue 3, November 2012, pp 381-395.

[66] Europol (2012), *Europol Review: General Report on Europol Activities*, The Hague, September 2012.

[67] Some elements can be found in, e.g.: Bruggeman, Willy (2006), *What are the options for improving democratic control of Europol and for providing it with adequate operational capabilities*, PE 378.274, Brussels, 1.2.2006; Mitsilegas, Valsamis (2006), *Police co-operation: what are the main obstacles to police co-operation in the EU?*, PE 378.273, Brussels, 1.1.2006; Scherrer, Mégie, Mitsilegas (2009), *The EU Role in Fighting Transnational Organised Crime*, PE 410.678, Brussels, 16.2.2009; Wills, Aidan, Vermeulen, Mathias et al. (2011), *Parliamentary oversight of Security and Intelligence Agencies in the European Union*, op. cit.

[68] European Commission (2011), *Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)*, COM(2011) 873 final, 12.12.2011.

[69] *Ibid*, Recital 1.

[70] *Ibid*, p. 3.

2.2.3.2 EU agencies and bodies as database managers

Besides the management of their own information systems (the EIS or FIS for instance), **EU bodies have also been tasked with the management of other databases**. As mapped out in the analytical table in Annex I, this is in particular the case of DG Home within the European Commission, which is at the time of writing still in charge of the management of Eurodac, SIS II and VIS. The management of these systems is expected to be transferred by December 2012 to the new European agency for the operational management of large-scale IT systems.[71] The seat of the agency is currently established in Tallinn, while the operational management of Eurodac, SIS II and VIS will take place in Strasbourg (with a back-up site in Sankt Johann im Pongau in Austria).

One question raised by the agency in view of the discussion so far is certainly **its future role in the possible, further expansion of the data and information exchange landscape** of EU JHA policies. 'Management', as framed by the agency's founding regulation, comprises "the preparation, development and operational management of large-scale IT systems in the area of freedom, security and justice" other than Eurodac, SIS II and VIS (Art. 1(3)). These tasks can only be undertaken by the agency on the basis of a legislative instrument. **The regulation suggests that the agency will have the capacity to monitor research and development in these areas beyond the scope of its tasks related to SIS II and VIS**, however (Art.8) and that **it would, upon the request of the European Commission, have the capacity to launch pilot schemes**. While the regulation provides in both cases for a mechanism requiring the agency to inform the Council and the European Parliament, **it does not include the possibility for these institutions to suspend monitoring activities or pilot schemes**. This suggests the need for specific monitoring mechanisms, especially as far as the European Parliament is concerned, to maintain proper oversight on the potential expansion of the already-widening landscape of data and information exchange in the field of JHA policies.

[71] European Parliament and Council of the EU (2011), Regulation (EU) No 1077/2011 of 25 October 2011establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286/1, 1.11.2011.

3. EU 'smart borders'

KEY FINDINGS

- 'Smart borders' aim at supplementing the SIS and VIS by logging movements in and out of the Schengen area (Entry/Exit System) and facilitating fast-track entry for pre-vetted registered travellers (Registered Traveller Programme).
- The foreseen costs of the planned EES and RTP have increased ten-fold since the proposals were first mooted in 2008. In the meantime, the degree to which 'smart borders' are necessary can be challenged considering the track record of these measures and the changes in scope, purpose and costs introduced over the past decade.
- 'Smart borders' systems are no longer only and mainly about borders: they involve the surveillance of foreigners travelling to, within and out of the Union.
- The planned 'Entry-Exit System' will lead to the fingerprinting of *all* third-country nationals entering the European Union, significantly expanding the EU's biometric information systems and increasing the amount of personal data accessible to law enforcement and security agencies.
- The planned 'Registered Traveller Programme', under which business and other frequent travellers would benefit from faster crossings, will institutionalise a two-tier border control system in the EU based on crude indicators such as wealth, nationality, employer and travel history.
- In envisaging the gradual replacement of border guards with 'Automated Border Control' gates, the planned 'smart borders' proposals may also pave the way for increased surveillance of EU citizens, whose movements could easily be recorded and stored in future.
- The proposed European Border Surveillance System (EUROSUR) is the most ambitious surveillance system ever envisaged by the EU with important implications for the protection of fundamental rights and democratic control that should be assessed in the same way as other 'smart border' proposals.

3.1 The 'smart borders' initiative

This subsection briefly presents the origins of the 'smart borders' initiative and details its contents. It furthers the discussion of reversibility, necessity and originality developed so far by suggesting that the blueprint for the current EU 'smart borders' initiative is strongly related to the policies of other countries in this regard, especially the United States, and that it has been circulating, under various guises, for quite a few years within the EU institutions.

3.1.1 EU and US policy initiatives related to 'smart borders'

As explained in the Introduction (section 1), the latest EU initiative in the field of external border controls, dubbed 'smart borders', **aims at supplementing the SIS and VIS by logging movement into and out of the Schengen area (EES) and facilitating fast-track entry for pre-approved registered travellers (RTP).** The tabling of these initiatives highlights the rapprochement between EU border control policies and the policy orientations initiated in the US under the George W. Bush administration. On both sides of the Atlantic, the principle is

similar: the collection of data on foreign nationals before they arrive at the border and the retention of that data to allow for further checks after they have entered. Formal identity checks still take place at the border itself, but the management and scrutiny of personal information begins at the point of applying for a permit or making an airline reservation and continues long after the traveller has returned home.

Once the 'front line' of border controls, the rows of desks staffed by immigration officers are now being supplanted by automated border control (ABC) gates capable of fingerprinting, digitally profiling and checking entrants against the information in their travel documents. Whereas the physical infrastructure of 'smart borders' – machine-readable passports, fingerprint checks, registered traveller programmes, ABC gates, etc. – has become increasingly visible in European airports, the way that the copious amounts of information that is generated is then retained and used remains largely hidden from view. This is highly problematic in terms of the potential impact on fundamental rights, privacy, data protection, due process, the presumption of innocence and democratic accountability. **In this sense, 'smart borders' are no longer only and primarily about borders: they involve the surveillance of foreigners travelling into, within and out of the Union**. Examined in the context of the EU JHA database landscape, and with a view to current and forthcoming proposals such as the EU PNR, **'smart borders' thus raise questions about the generalisation of surveillance through data and information ('dataveillance').** This phenomenon is examined in more details under the heading of 'statistical discrimination' in section 4.

In the EU context, the current discussion on smart borders began in February 2008, when the European Commission proposed the development of a comprehensive 'border package' for the EU comprised of an Entry-Exit System, a Registered Traveller Programme, Automated Border Control gates and a European Electronic System of Travel Authorisation.[72] Although this initiative has now been cast on a separate track, the 2008 'border package' was accompanied by a proposal to develop an EU external border surveillance system (EUROSUR).[73] The idea of establishing an EU 'Entry-Exit System' (EES), loosely modelled on the 'US VISIT' system, was first given serious consideration in 2004, as part of discussions about the design of the future Visa Information System (VIS).[74] The idea was to collect personal data (including fingerprints) from all visa applicants before they arrived in the EU so that their identities could be checked upon entry (as now happens with VIS), and then to verify and record their exit from the EU for the purpose of demonstrating compliance with immigration rules and helping identify 'over-stayers' (a function VIS does not yet have).

Among the reasons it was decided **not to develop an EES alongside VIS is that it would only have covered third-country nationals (TCNs) subject to EU visa requirements** – data on persons from countries who benefit from the EU visa waiver, along with persons holding long-term visas or residence permits, would not have been included. There was also marked concern about the substantial time and resources required to collect and store biometric data from all TCNs arriving at the EU's external borders and record all exits. Thus, in 2008, the European Commission linked the EES to proposals to establish an EU Registered Traveller Programme and Electronic System of Travel Authorisation (ESTA); the former would speed entry for *bona fide*, pre-vetted (mainly business) travellers while the latter would enable the collection of data

---

[72] European Commission (2008), *Preparing the next steps in border management in the European Union*, COM(2011) 69 final, 13.2.2008.

[73] European Commission (2008), *Examining the creation of a European Border Surveillance System (EUROSUR)*, COM(2011) 68 final, 13.2.2008.

[74] European Policy Evaluation Consortium (2004), *Study for the extended impact assessment of Visa Information System*, December 2004.

(and vetting) of travellers not subject to the EU visa requirement or registered in the VIS. As detailed below, however, the 2011 'smart borders' communication discards the establishment of an EU-ESTA and advocates the creation of an EES that would record the entries and exits of so-called 'non-visa nationals'.

3.1.2 Towards a legislative proposal on 'smart borders'

The Commission's 'smart borders' Communication of 2008 was welcomed by the Council which, in order to assist the Commission in conducting an impact assessment and developing a full legislative proposal, issued two questionnaires to the Working Party on Frontiers in 2009. The first sought to assess the appetite among the member states for a 'smart border' system centred on an EES;[75] the second requested statistics regarding border crossings and the entry and exit of TCNs.[76]

The Commission was scheduled to present the legislative proposal by mid-2011, with a view to the systems becoming operational in 2015, but the Polish Presidency clearly harboured doubts about the necessity or effectiveness of smart borders. The informal JHA ministerial in Sopot in July 2011 called for a "shared understanding" between the Commission and the member states "before embarking" on such an ambitious proposal and invited ministers to reflect upon "the added value in light of the technological implications (including in relation to data protection) and the cost".[77]

Instead of its planned legislative proposal, the Commission responded in October 2011 with a new Communication not intended to "prejudge any future specific proposals", which would be accompanied by a full impact assessment in due course.[78] **The substantial difference between the 2008 and 2011 Communications was that the estimated costs of the Entry-Exit System and Registered Traveller Programme had increased tenfold**: from €135 million to €1.335 billion. Meanwhile, plans to introduce an Electronic Travel Authorisation System (for third-country nationals not subject to the EU visa requirement) did not feature in the 2011 'smart borders' communication and have apparently been shelved. Finally, in February of this year, the Danish Presidency hosted a conference on "Innovation in Border Management" to provide further guidance to the Commission in its deliberations.[79]

The move towards a legislative proposal on 'smart borders' highlights the relevance of the discussion on reversibility, necessity and originality we have examined so far. The EES warrants further scrutiny in this regard. The degree to which **its establishment is the inevitable outcome of existing EU policies on external border control, migration and visas can be challenged** when taking into consideration the track record of this particular measure and the changes in scope, purpose and costs that it has undergone over the past decade. Considering the components of the 'smart borders' initiative as an irreversible process, in the meantime, has strong implications for the decision-making process. We will detail the matter of costs in depth at a later stage (see point 3.2.5), but it is worth underlining that **despite the absence of a formal**

---

[75] Council of the EU (2008), *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 13403/08, Brussels, 24.9.2008; Council of the EU (2009), *Questionnaire on the possible creation of a system of electronic recording of entries and exits of third country nationals in the Schengen area*, 8552/09, Brussels, 21.4.2009.

[76] Council of the EU (2009), *Results of the data collection exercise*, 13267/09, Brussels, 22.9.2009.

[77] Polish Presidency of the European Union (2011), *Conclusions of the Informal Meeting of the Justice and Home Affairs Ministers in Sopot, 18–19 July 2011*: *Smart borders in the Schengen space*.

[78] European Commission (2011), COM(2011) 680 final, *op. cit.*

[79] Danish presidency of the European Union (2012), *Conference on Innovation Border Management*, 02-03.02.2012: http://eu2012.dk/en/Meetings/Conferences/Feb/Konference-om-innovativ-graenseforvaltning.

legislative proposal or a firm political commitment on the part of national governments, the Commission has already earmarked €1.1 billion for the development and implementation of 'smart borders' from the draft EU Internal Security Fund 2014-20.[80] It argues that it has to do this so that the money is available if the member states wish to implement 'smart border' systems during the next multi-annual financial framework. It may also, however, enable substantial EU investments to be made prior to or irrespective of future decisions regarding EU legislation.

This observation is not limited to the 'smart borders' initiative, but appears to be a consistent pattern in EU JHA policies. This is indeed precisely what happened with EUROSUR after the strategic guidelines for the External Borders Fund 2007-13 encouraged member states to use the fund for "national components of a European Surveillance System". By the time the EUROSUR legislation was formally proposed in December 2011, 16 out of the 18 member states located at the southern and eastern external borders had established their EUROSUR National Coordination Centres; the majority were already operational.[81] In such circumstances, the scope for European and national parliaments to raise any substantive objections to the EUROSUR legislation was greatly diminished.

The use of financial instruments such as the Seventh Framework Programme for Research (FP7) and the various (existing and forthcoming) EU home affairs funds by the European Commission to pursue predefined policy objectives is now having a significant impact on the EU legislative agenda. **In these circumstances the European Parliament is advised to establish monitoring mechanisms that allow the scrutiny of these practices, the meaningful review of what has been spent, and how it has influenced policy and legislative practices.**

3.2 The foreseen systems

This subsection details each of the three data and information exchange schemes envisaged in the 'smart borders' Communication of 2011. In order to continue the discussion on reversibility, necessity and originality, it starts with the examination of the one system that in fact has been discarded by the European Commission, namely ESTA. Read through ESTA, the link between existing and 'smart borders' systems and the necessity of the EES and RTP can indeed be discussed critically.

3.2.1 Electronic System of Travel Authorisation

An Electronic System of Travel Authorisation (ESTA) provides for the pre-screening of travellers not subject to a visa requirement. It has been pioneered in the United States as part of its Visa Waiver Programme and requires travellers to submit an electronic application at least 72 hours before travelling to the United States. ESTA applicants are then screened against national security 'watch lists' so that individuals of interest to the authorities can be identified prior to departure and prevented from boarding inbound aircraft. Australia also operates an ESTA scheme as part of its Advance Passenger Processing system.

---

[80] European Commission (2011), *Building an open and secure Europe: the home affairs budget for 2014-2020*, COM(2011) 749 final, 15.11.2011. See further European Commission (2011), *Proposal for a Regulation of the European Parliament and of the Council establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa*, COM(2011) 750 final, 15.11.2011.

[81] European Commission (2011), *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR),* SEC(2011) 1536 final, 12.11.2011, pp. 15–16.

There is understandably some confusion between ESTA programmes and Advance Passenger Information (API) systems. The former requires selected travellers to obtain formal authorisation from competent state authorities; the latter places an obligation on carriers to collect specific information from travellers (including name, date of birth, nationality, passport number, expiry date, issuing authority, etc.) and communicate it to those authorities prior to the departure of their aircraft. While API data may also be vetted by security services to identify suspicious or wanted persons and/or to prevent departure, no formal system of travel authorisation is provided to the individuals concerned. API systems are linked to Passenger Name Records (PNR), which also allow states to vet or profile travellers. Most EU states now require some form of Advance Passenger Information. Again, from the citizen's perspective, it is becoming increasingly difficult to understand what data are being collected by whom and for what purposes.

In its 2008 Communication on smart borders, the Commission suggested that the EU could introduce an ESTA for "third-country nationals not subject to the visa requirement" who "would be requested to make an electronic application supplying, in advance of travelling, data identifying the traveller and specifying his/her passport and travel details".[82] This data would be used "for verifying that a person fulfils the entry conditions before travelling to the EU, while using a lighter and simpler procedure compared to a visa".

A feasibility study on an EU ESTA was produced by an external contractor in February 2011.[83] It considered four options: an ESTA for all visa-exempted TCNs, an ESTA for certain visa-exempted TCNs only, an ESTA scheme that worked in combination with a wider 'e-visa' system covering all entrants, and a gradual substitution of the visa requirement itself in favour of a comprehensive ESTA scheme. The study ultimately recommended that that "the establishment of an EU ESTA would not, under any of the four options identified, respond to fully unambiguous, well-identified and fully understood needs and problems at this stage", although it noted that in the long-term, when VIS and EES were both up-and-running, an EU ETSA in the form of an electronic visa application system "could bring a number of tangible benefits for visa authorities as well as for travellers".[84] However, by the time feasibility study was published in 2011, the Commission had already discounted the option of establishing any kind of EU ESTA in favour of a European Entry-Exit System and Registered Traveller Programme.

3.2.2 Entry/Exit System

According to the Commission's Communication of 2008, an EU Entry-Exit System would have the general purpose of identifying 'over-stayers' – non-EU nationals who enter legally with a valid travel document or visa and then fail to leave upon expiration of their permitted stay. While it is often claimed that such persons comprise the largest category of 'illegal migrants' in the EU, no accurate statistics exist. Indeed the Commission suggests that the 'added value' of the EES is that it will be able to provide more accurate information about patterns of overstaying.

The EES would work by registering the time and place of entry and exit of all TCNs admitted for a short stay (up to three months). This will require amendments to the Community Code on

---

[82] European Commission (2008), COM(2008) 69 final, *op. cit.*

[83] Price Waterhouse Coopers (2011), *Policy study on an EU Electronic System for Travel Authorisation (EU ESTA)*

Final Report, February 2011.

[84] *Ibid.*, pp. 27-28.

the rules governing the movement of persons across the borders (the Schengen Borders Code - SBC), which provides a set of harmonised rules and procedures for the crossing of the external borders of the EU.[85] In cases where a person's stay expires and no exit data are captured by the EES, some kind of 'alert' would be sent to the national authorities so that 'appropriate measures' can be taken.[86] While no sanction has yet been specified, it is assumed that this will include fines and/or issuing an expulsion order. It is also possible that the EES could be *de facto* linked to the Schengen Information System for the purposes of apprehending 'over-stayers' (see further section 3.3.1. below).

It is as yet unclear exactly what data would be stored in the ESS but this will have to include at least the information necessary to trace the identity, travel document, place and date of entry of any 'over-stayers'. In its 2011 Communication, the Commission favoured the establishment of the EES in stages with alpha-numeric data such as name, nationality and passport number collected initially, with fingerprints and photographs introduced at a later stage.[87] However, a majority of member states that have expressed a position on the issue wish to see biometric data included from the outset.[88]

Third-country nationals account for almost half of the 300 million people estimated to cross the external borders of the Schengen area every year. With the planned EU Entry-Exit System, their data would be stored in a central database fed by information collected by computer terminals at external border-crossing points. Thus, as with other large-scale EU migration databases, the bulk of the overall costs outlined above lie in upgrading border control systems in the member states.

The EES will share the Biometric Matching System (BMS) developed for the VIS and the Schengen Information System II.[89] The BMS is used to verify the identity of visa holders (so-called 'one-to-one' checks) or check individual prints against either database ('one-to-many' checks). It would still of course be much simpler and cheaper to introduce an entry-exit functionality within VIS but this would fail to capture those TCNs who arrive from countries not subject to the EU visa requirement.

It is not yet clear how long data might be retained in the EES. The Commission has said data could be kept in order to establish and map 'travel patterns', suggesting the VIS standard of five years could be used. Others have argued that it would be disproportionate and potentially unlawful to retain personal data on individuals who have entered and left the EU in full accordance with immigration rules.[90]

---

[85] European Parliament and Council of the EU (2006), Regulation (EC) No 562/2006 of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders ("*Schengen Borders Code*"), OJ L 105/1, 13.4.2006.

[86] European Commission (2008), COM(2008) 69 final, *op. cit*., p. 8.

[87] European Commission (2011), COM(2011) 680 final, *op. cit*., p. 9.

[88] Council of the EU (2011), *Communication from the Commission to the European Parliament and the Council: "Smart borders - options and the way ahead" - Summary of discussions*, 17706/11, 29.11.2011, p. 2.

[89] The Biometric Matching System (BMS) is an information search engine that can match biometric data from visa applications, identity management systems and policing systems for EU member countries. The BMS is designed to enable justice and immigration authorities to deal with security and other issues related to terrorism, organized crime, illegal immigration, visa shopping, identity theft and fraud. The BMS database will be able to store the fingerprints of up to 70 million people and process more than 100,000 verification and identification requests per day. See Accenture press release, *Accenture and Sagem Défense Sécurité Win Prime Contract for European Commission's Biometric Matching System*, 20.10.2008.

[90] See for example Hayes, B. and Vermeulen, M. (2012), *Borderline: The EU's New Border Surveillance Initiatives*, Berlin: Heinrich Böll Foundation, 2012.

The newly established EU Agency for Large-scale IT Systems would be responsible for the development and management of the EES and access would logically be granted to the competent immigration services of the member states. In its Communication of 2008, the Commission had suggested that "law enforcement authorities" could be granted access to EES data "in exceptional circumstances… with good cause".[91] However, several member states have called for such agencies to be granted access for general policing purposes while 11 member states implementing national entry-exit systems already make, or envisage making, the same provision.[92]

3.2.3 Registered traveller programme

Registered Traveller Programmes (RTPs) are designed to speed border-crossing for pre-vetted or 'bona fide' travellers. They are based on automated identity checks and border-crossing gates, reducing or removing the need for border guards to check travel documents. Only four member states currently have RTPs which are limited to the busiest airports.[93] Airports in several other states are introducing automatic border control (ABC) gates independently of RTPs.[94]

Within the EU 'smart borders' package, the RTP is conceived as a means to compensate for longer procedures for registering travellers in the planned Entry-Exit System. The EU's RTP scheme would be voluntary and those applicants who are approved as 'bona fide' travellers would be able to use ABC gates at the EU's external borders. The Commission estimates that this would cut the time spent queuing to "below 30 seconds" – a privilege that RTP members would pay for.[95] The Commission hopes that "4-5 million travellers per year" would use the EU's RTP and that the revenues generated would "lay the basis for enhanced investments in automated border control technologies at major border crossing points."[96]

In 2008 the Commission identified various factors that could be used to determine which travellers could be identified as 'low risk' and suitable for inclusion in an EU RTP. This includes travelling frequently to the Schengen area for legitimate reasons (for instance travelling on business), a reliable travel history (the person respects the conditions for their length of stay on each occasion), proof of sufficient means of subsistence and possession of a biometric passport.[97] Applicants would also be checked against national and international 'watch lists' to ensure that they are not considered a threat to public policy, internal security, public health or international relations of any of the member states.[98] According to the Commission, "other criteria may be imposed."[99] At the informal JHA Council in July 2011, the Council hinted that the vetting criteria could be aligned with the criteria for multiple-entry visa holders.[100]

---

[91] European Commission (2008), COM(2008) 69 final, *op. cit.*, p. 27.

[92] European Commission (2011), COM(2011) 680 final, *op. cit.*, p. 7.

[93] These systems are *Parafes* in France, *ABG* in Germany, *Privium* in the Netherlands and *Iris* in the United Kingdom.

[94] For example *RAPID* in Portugal and the Automated Border Control gates in the United Kingdom and Spain.

[95] European Commission (2011), COM(2011) 680 final, *op. cit*., p. 12.

[96] *Ibid*.

[97] European Commission (2008), COM(2008) 69 final, *op. cit*., p. 6.

[98] *Ibid*., p. 7.

[99] European Commission (2008), *Preparing the next steps in border management in the European Union – Summary of the Impact Assessment*, SEC(2008) 153 final, 13.2.2008, p. 62.

[100] Polish Presidency of the European Union (2011), *op. cit.*, p. 3.

Upon arrival at the ABC gates, a document reader would check the biometrics of registered travellers against those stored by the EU RTP. Those systems already operating in the member states use iris scans or fingerprints. The Commission and those member states that support an EU RTP are understood to want to use both fingerprints and facial scans. While it might be possible to develop interoperable, national systems linking only those states wishing to introduce RTPs, a central EU system is planned.[101] In its 2011 Communication, the Commission suggested that the data of registered travellers could either be stored in a central database or on a token issued to the individual RTP member, or a combination of both, in which case the token would only contain a unique identifier such as a membership number.[102] A majority of member states expressing a position on these options prefer the centralised storage of data.[103]

It is not yet clear which agencies would have access to the data held in the EU RTP, although this would logically include competent immigration services and those security agencies responsible for checking applicants against 'watch lists'. It is not known at this stage if law enforcement agencies will be granted routine access to RTP data as seems likely in respect to the EES.

3.2.4 The rationale for 'smart borders'

The basic principle behind 'smart borders' is the automation of the processes involved in border controls and immigration checks; in essence the replacement of human checks by computer checks. However, in automating border-crossing procedures, a vast amount of personal data can be collected and retained for a range of purposes, including the profiling of travellers (in attempts to identify 'suspicious' persons), cross-checks against national security and police 'watch-lists', creating of registers of entrants and facilitating the surveillance of movement.

In addition to automated data collection and processing at border-crossing points, the concept of 'smart borders' also encompasses the introduction of detection technologies aimed more broadly at preventing unauthorised entry and residence. This includes, for example, the use of automated surveillance and analysis systems in attempts to control border areas, to identify suspicious vehicles, vessels or persons, and to autonomously track and profile them. The draft EUROSUR legislation appears to provide for the continuous development and implementation of such technologies in order to create an ever-more comprehensive 'situational picture' through continuous surveillance of large areas outside of EU territory (see section 3.3.2 below). Considered alongside the expanded mandate for Frontex to target activities relating to illegal immigration within the EU and all of the JHA databases already geared to controls on asylum applicants and legal entrants and residents, 'smart borders' are institutionalising surveillance across whole continents.

'Smart borders' derive their perceived legitimacy from assumptions about efficiency and security; the premise is that they benefit travellers by deploying new technologies and enhance the effectiveness of border checks through the introduction of automated processes. The Entry-Exit System is at the heart of the 'smart border' plans for the EU. The extent to which the EES will either benefit travellers or enhance security is, however, still very much open to debate. Primarily, it is clear that collecting biometric information and recording the entry-and-exit of all third-country nationals crossing the EU's external borders will *increase* the time that travellers spend at immigration controls, regardless of the extent to which new technologies are able to speed this process.

---

[101] European Commission (2011), COM(2011) 680 final, op. cit., p. 8.

[102] *Ibid*., pp. 8–9.

[103] Council of the EU (2011), 17706/11, *op. cit.*, p. 2.

The legitimacy of the EES is thus dependent on its value as a security tool but as yet even the Commission appears unconvinced of its merits in this respect. It has previously argued that collecting entry and exit data will assist in identifying 'over-stayers' and collecting reliable statistical data on the extent of the phenomenon. However, without a concrete link to arrest and expulsion procedures (see section 3.3.1 below), the EES is only likely to identify 'over-stayers' at the point at which they attempt to exit the Schengen area, which is too late to prevent unauthorised residence as it logically marks the end of any such stay. In this context the EES would create little more than an extremely expensive mechanism for gathering migration statistics.

Furthermore, it is understood that the Commission services responsible for developing the forthcoming EES proposal have failed to convince the Commission's Impact Assessment Board about the purpose of the system as described above, or the necessity of collecting biometric data from third-country nationals not subject to a visa requirement. The Commission services committed to the introduction of the EES now have little choice but to 'beef up' their proposal, likely by including biometrics in the system from its inception, making a stronger case for EES as a policing tool, and granting law-enforcement agencies access to EES data.

While concerns may be raised about the proportionality and legitimacy of a system that effectively creates a police record on all visitors to Europe, not least in the light of the European Court of Human Rights' judgment in *S & Marper* v *United Kingdom*,[104] it is difficult to escape the conclusion that the main 'value' in the EES has always been the collection of biometric data to complement that collected by Eurodac and VIS. In this context, the problem of visa 'overstaying' is being used to justify what effectively amounts to a policy of extending mandatory fingerprinting from all asylum and visa applicants to all TCNs attempting to enter the EU. Nevertheless, it is important to note that if the rationale for 'smart borders' is to increase EU security by preventing the entry or identifying the presence of suspicious or dangerous travellers, this could be achieved through much cheaper and less-intrusive systems such as ESTA or API, which do not require the collection and retention of biometric data.

Whereas the Commission is likely to attempt to justify any proposed EES on security grounds, the rationale for the planned Registered Traveller Programme is based solely on efficiency. The Commission recognises that collecting or checking biometric data from an increasing number of travellers arriving at the EU's external borders will significantly increase waiting times and is concerned that this could frustrate business and other frequent travellers. The proposed EU RTP would allow this group of persons – subject to vetting by the security services – to circumvent lengthier border-crossing procedures in return for payment. The revenues that the Commission envisages that this will generate help fund the introduction of automated border-crossing gates. The Commission argues that ABC gates will in turn lead to a substantial cost-saving by reducing the number of human border guards required to conduct such checks.

Several important shortcomings have been identified with regard to this approach. Primarily any EU RTP will in effect introduce a two-tier system whereby a select few will benefit from faster crossings whereas the vast majority of travellers will face lengthier border checks. It was also create a *de facto* division between 'low-risk' and 'high-risk' travellers based on crude and potentially discriminatory indicators such as wealth, nationality, employer and travel history.

---

[104] According to established case law of the European Court of Human Rights, the mere storing of data amounts to an interference with the right to privacy. In the *S. and Marper* case, the Court ruled that fingerprints and photographs contain unique information that is "capable of affecting the private life of an individual" and that retention of this information without the consent of the individual concerned "cannot be regarded as neutral or insignificant". European Court of Human Rights (2008), Case *S. and Marper v the United Kingdom*, ECHR 1581, Applications nos. 30562/04 and 30566/04, Judgment, 4 December 2008, para. 84.

There are also obviously flaws from a security perspective insofar as people intending to commit criminal acts in the EU may still be perfectly capable of obtaining RTP accreditation.

Finally, if ABC gates are rolled-out across the EU to facilitate the planned Registered Traveller Programme, some degree of 'scope creep' is inevitable. Those member states that have already introduced ABC gates in the absence of any RTP programme have done so to speed-up border crossings for EU citizens holding technologically-compatible passports. In envisaging the gradual replacement of border guards with ABC gates, the 'smart border' proposals may also pave the way for increased surveillance of EU citizens, whose movements could easily be recorded via ABC gates and incorporated into national entry-exit systems.[105]

3.2.5 The costs

As noted above, the foreseen costs of the planned EES and RTP have increased ten-fold since the proposals were first mooted in 2008 and the "estimated costs of the centralised entry/exit and Registered Traveller Programme system [were] approximately 20 million euro, spread out over 2-3 years and the annual maintenance and operational costs approximately 6 million euro." The Commission explained that it would cost a further €35 million to implement the EES and RTP in the member states, "but [this] could vary greatly depending on the number of automated gates that would be implemented. One automated gate unit costs approximately 35,000 euro."[106]

When the Commission revisited the potential costs of the EES and RTP in 2011, it reported that the development of the central EES and RTP and their national interfaces could be in the order of €400 million, with annual operating costs of €180 million per year for the first five years.[107] The Commission also estimated that if the EES and RTP are built on the same 'technical platform' (i.e. as a single rather than disparate systems), this could bring the total cost down to under €1 billion.

Insofar as the potential costs of any new systems must be weighed against the envisaged benefits and sheer ambition of the proposals, many commentators have pointed to the US experience with the US VISIT programme. As the European Data Protection Supervisor (EDPS) has noted, by 2008 this system had cost more than $1.5 billion but only led to 1,300 entry refusals, equating to more than $1 million per refusal.[108] Moreover, despite collecting fingerprint data from all non-NAFTA nationals entering the US, US VISIT is only able to record entry data. It has long been planned to record exit data as well but the Department of Homeland Security (DHS) has been unable to convince the Government Accountability Office (GAO) that these plans are viable, despite repeated attempts to do so. The GAO has currently identified planning and implementation problems related to the 'exit' component of US-VISIT.[109] Over the past three years, and following the attempted bombing of an airline on 25

---

[105] The Commission explicitly foresees that EU citizens could 'benefit' from automated gates when crossing the external borders, see European Commission (2008), COM(2008) 69 final, *op. cit*., p. 7.

[106] European Commission (2008), *Preparing the next steps in border management in the European Union – Summary of the Impact Assessment*, SEC(2008) 154 final, 13.2.2008.

[107] European Commission (2011), COM(2011) 680 final, *op. cit.*, p. 10.

[108] Cited in Peers, Steve (2008), Proposed new EU Border Control Systems, PE 408.296, Brussels, June 2008, p. 9.

[109] GAO (2007), *Homeland Security: US-VISIT has not fully met expectations and longstanding programme management challenges need to be addressed*, GAO-07-4997T, Washington, D.C., February 2007; GAO (2007), *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain*, GAO-07-346, Washington D.C., May 2007; GAO (2009), *Homeland Security: Key US-VISIT Components at Various Stages of Completion, but Integrated and Reliable Schedule Needed*, GAO-10-13, Washington D.C., November 2009.

December 2009 in Chicago, the GAO has become increasingly critical of the methods followed by the DHS as well as by the outcome of its work. In an August 2010 report, it questioned the relevance of two pilot studies on US-VISIT's exit component that the DHS had been required to implement by the 2009 Consolidated Security, Disaster, Assistance and Continuing Appropriation Act of September 2008.[110] The testimony of a high-level GAO official before the US House of Representatives' Subcommittee on Border and Maritime Security in September 2011 highlights that without a "master schedule [*for the implementation of the exit component of the US-VISIT programme*] that was integrated and derived in accordance with relevant guidance, DHS could not reliably commit to when and how it would deliver a comprehensive exit solution or adequately monitor and manage its progress towards this end".[111]

The European Commission, by contrast, is hoping to deliver the EES and RTP for a much lower cost than the US VISIT scheme. Meanwhile, the scope of the envisaged EES/RTP scheme is much more ambitious: the US has a single federal border-control system, while EU national authorities in charge of this issue amongst the participating Schengen states have diverse capacities and competencies, and arguably more dispersed, heterogeneous and numerous crossing points to monitor between them.

This observation is all the more important as the EU has already invested more than €200 million in research and development of smart borders and border surveillance technologies from its FP7.[112] This includes a host of prototype detection technologies for EUROSUR and two large-scale demonstration projects for EU ABC gates.[113] As documented in previous studies for the European Parliament,[114] EU R&D funding has provided European industry with a platform to develop and showcase technological options, including for 'smart borders', thus institutionalising the dialogue between policy-makers, practitioners and technology suppliers. Multinational defence and security contractors such as *Finmecannica-SELEX*, *Indra Sistemas*, *Sagem*, *Thales* and *EADS* have played a particularly prominent role.[115] Within this process, discussions about the necessity and impact of new technologies have been sidestepped or substituted with industry-friendly concepts such as 'privacy by design'.

3.3 Smart borders and JHA databases

3.3.1 Smart borders, VIS and SIS/SIS II

The expected EU proposals on EES and RTP have various implications for the way in which the Visa information System and potentially the Schengen Information System (and SIS II) are used in practice. Unfortunately these relationships cannot be clarified until the formal Commission

---

[110] GAO (2010), *Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options*, GAO-10-860, Washington D.C., August 2010.

[111] GAO (2011), *Visa Security: Additional Actions Needed to Strengthen Overstay Enforcement and Address Risks in the Visa Process – Statement of Richard M. Stana, Director Homeland Security and Justice Issues*, GAO-11-910T, Washington D.C., 13.9.2011, p. 10.

[112] Hayes, B. and Vermeulen, M. (2012), *Borderline*, op. cit., pp.59-66.

[113] The two large-scale demonstration projects for EU ABC gates are FASTPASS and ABC4EU. They are expected to commence in 2013.

[114] Bigo, D. and Jeandesboz, J. (2008), *Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*, PE 393.289, Brussels, May 2008; Burgess. J.P. and Hanssen, M. (2008), *Public Private Dialogue in Security Research*, PE 393.286, Brussels, May 2008; Jeandesboz, J. and Ragazzi, F. (2010), *Review of security measures in the Research Framework Programme*, PE 432.740, Brussels, October 2010.

[115] Hayes, B. and Vermeulen, M. (2012), *Borderline*, op. cit., pp.60-66.

proposals are produced. The analytical table in Annex I provides an overview of the main components of those databases.

As noted above, the EES will share the Biometric Matching System developed for VIS and SIS II. It is also possible that the RTP will share the BMS as well; this will certainly be the case if the cost-saving option of developing the ESS and RTP in tandem is pursued. In the context of 'one too many' searches, where law enforcement agencies attempt to match fingerprints to their holders, a single interface could then be provided to the fingerprints of hundreds of millions of TCNs. It is important to recognise here that centralising access to different datasets can achieve the same goal as interlinking the databases themselves (c.f. the recent proposals to grant law enforcement agencies access to Eurodac data).

There are likely to be more explicit links between VIS and EES. Since the EES will include the entry and exit data of *all* third-country nationals, it is logical that data related to TCNs who are subject to a visa requirement will be interoperable with the VIS system.[116] Indeed, the Commission has suggested that a fully operational and developed VIS is "a prerequisite for the implementation of a Smart Borders system",[117] though it is unclear why the Commission does not want to wait until the VIS is fully functional and review the operation of the system before attempting to establish the EES.

Nor is it clear how 'overstay' alerts will be issued and acted upon in the event that an individual registered in the EES fails to exit the EU in accordance with the terms of their visa or visa waiver. The Commission has already explained that 'alerts' will automatically be issued to the competent national authorities when an individual's scheduled exit has not been captured by the EES; since persons 'overstaying' their visa may be liable for a fine and/or expulsion, it is logical that these alerts will be sent to the responsible authorities. But as the Treaty provides for the free movement of Schengen visa holders, what if the 'over-stayed' has left the member state through which they entered and is now residing elsewhere in the EU? The Commission has thus far remained silent on this issue, but from a law enforcement perspective it may be desirable to issue 'over-stayer' alerts through the Schengen Information System (or SIS II once it is up-and-running).

If the architects of the EES do ultimately intend for *de facto* arrest warrants for 'over-stayers' to be issued via the SIS/SIS II, it is imperative that stringent safeguards are introduced. It must be questioned from the outset whether it is lawful or proportionate to issue arrest warrants for what are in most member states civil/administrative offences, but in the same vein certain member states have long been registering rejected asylum-seekers and persons refused entry to their territory in the SIS *en masse*, with the effect that the individuals concerned are effectively subject to an EU-wide entry ban. **The European Parliament should therefore seek to clarify the envisaged relationship between EES, VIS and SIS II at the earliest opportunity.**

3.3.2 Smart borders and EUROSUR

The legislation formally establishing EUROSUR, the EU Border Surveillance System, was proposed in December 2011.[118] However, as noted above, by this time the development of

---

[116] Member states also appear to favour this option; see Council of the EU (2011), doc. 17706/11, *op. cit.*, p. 2.

[117] European Commission (2011), COM(2011) 680 final, *op. cit*., p. 7.

[118] European Commission (2011), *Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)*, COM(2011) 873 final, 12.12.2011.

EUROSUR was already well underway.[119] The primary purpose of EUROSUR is to improve the 'situational awareness' and reaction capability of Frontex and the member states to prevent irregular migration and cross-border crime at the EU's external land and maritime borders. In practical terms, the Regulation will extend the obligations on Schengen states to conducting comprehensive '24/7' surveillance of land and sea borders designated as 'high-risk' in terms of unauthorised migration and mandate Frontex to carry out surveillance of the open seas beyond EU territory and the coasts and ports of northern Africa.[120]

Although EUROSUR has been developed independently of the other elements of the EU 'smart borders' package, the principle of expanding surveillance from the actual border to points of departure and transit of migrants is the same – the former focusing on the unauthorised/undocumented, the latter on legal/'bona fide' travellers. There are striking similarities too in the way in which the security and defence industry has been subsidised to support the development and implementation of EUROSUR,[121] whereas the European and national parliaments were not consulted until the technical development of the system was well underway, presenting them with something of a *fait accompli*. From the perspective of democratic control and legitimacy, it is disconcerting that while large-scale JHA information systems such as the Schengen and EUROPOL Information Systems were developed on the basis of 'primary' (enabling) and 'secondary' (implementing) legislation, which was the subject of at least some public debate, in the case of EUROSUR this method was substituted for a technocratic process that allowed for substantial public expenditure to occur well in advance of the legislation now on the table.

EUROSUR envisages the use of coastal radar, satellite tracking systems, 'drones' (or unmanned aerial vehicles) and autonomous targeting systems to identify, detect and follow small vessels bound for EU territory. There is potentially no limit to the types of surveillance technologies that may be deployed as part of EUROSUR and so-called 'function creep' appears to have been built-in to the system. Developed on the premise of enhancing control of EU external borders, EUROSUR may ultimately be incorporated into a much broader information system that could be used for "Maritime Safety (including Search and Rescue), Maritime Security and prevention of pollution caused by ships; Fisheries control; Marine pollution preparedness and response; Marine environment; Customs; Border control; General law enforcement [and] Defence".[122] In these scenarios, EU citizens travelling by or working at sea would then be every bit as likely to be placed under routine surveillance as migrants and refugees bound for Europe.

Despite its potential scope, the draft EUROSUR Regulation lacks comprehensive data protection safeguards. It is argued by Frontex and the European Commission that these are unnecessary because EUROSUR will not collect massive amounts of personal or biometric data, or result in the establishment of a centralised database that stores such information, but it is clear that personal data could still be processed in various ways. As noted in section 2.1 above, the decentralised *appearance* of EUROSUR and the processing of predominantly 'non-personal' data is perceived by policy-makers as justifying a lower level of democratic control and fundamental rights protections than 'traditional' law enforcement databases. **Yet**

---

[119] In its February 2008 Communication on EUROSUR the European Commission announced that it was to begin developing the EUROSUR system immediately under an eight-step 'Roadmap'. See European Commission (2008), COM(2008) 68 final*, op. cit.*

[120] For a comprehensive examination of the development and implementation of the EUROSUR system see Hayes, B. and Vermeulen, M. (2012), *Borderline*, op. cit.

[121] *Ibid*. pp. 55-72.

[122] European Commission (2010), *Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain*, COM(2010) 584 final, 20.10.2010.

EUROSUR represents what is certainly the most ambitious surveillance system ever envisaged by the European Union, whether measured in terms of geographical or technological scope or levels of 'interoperability'. From this perspective EUROSUR should be the subject of much greater debate, concern and safeguards. It is also regrettable that EU policy-makers have apparently chosen to ignore failed attempts by the US to create a similar system covering the US-Mexico border. 'SBI-net' was supposed to establish a 'virtual fence' using a complex network of high-tech surveillance equipment but funding for the $3.7 billion project was frozen in 2010.[123]

[123] See further Hayes, B. and Vermeulen, M. (2012), *Borderline*, op. cit., pp.70-72.

4. Challenges of JHA databases and smart borders: data protection, privacy, non-discrimination

KEY FINDINGS

- The first legal challenge posed by JHA databases relates to the principle and fundamental right of privacy. Independently from the personal character of the information collected and/or processed, databases are in tension with the general EU principle of privacy, which extends beyond data protection to the wider right to private life as envisaged in the Charter and also includes 'anonymised' or 'operational' data. The conditions under which de-personalised data can or could be re-personalised by law enforcement authorities are of utmost relevance.
- JHA databases have a very broad personal scope as they cover a wide range of individuals with a variety of legal statuses in accordance with EU law. This leads to a blurring of the targeted individuals as data subjects and to negative repercussions over the principle of legal certainty. They also fail to take into account the vulnerability inherent to certain groups of travellers and foreigners. Non-EU citizens can experience even more difficulties as regards the right to be informed, to access their data and to effective remedies. This risk is further increased due to the existence of multiple EU systems working on different EU AFSJ policy areas.
- An additional legal challenge pertaining to JHA databases and 'smart borders' concerns the actual necessity surrounding the establishment of JHA databases, which lies at the heart of the proportionality principle test. It is at present far from clear to which extent these systems pass satisfactorily the necessity test as applied by the European Court of Human Rights and the Court of Justice of the European Union.
- While nationality and legal status may not be considered as connecting factors for activating the EU non-discrimination system of protection for TCNs, any person (independently of his/her migration administrative status) is a beneficiary of the general non-discrimination protection which constitutes a well-established principle in the EU legal regime now expressly enshrined in Article 21 of the EU Charter. These apply equally to EU citizens and foreigners.
- It is challenging to distinguish discrimination on the basis of race and ethnic origin, from that of 'nationality'. The exclusion of nationality discrimination in the scope of the Race Equality Directive is somehow at odds with a reality where discrimination of TCNs is multi-grounded or multi-faceted. How can border controls be carried out in such a way that they discriminate only on grounds of nationality, and without using nationality to justify indirect discrimination on prohibited grounds?
- JHA databases and smart borders work on the basis of 'automated decision-making' parameters, which correspond with what has been denominated as 'profiling' or 'predictive data-mining'. Profiling is used 'to select' a group of people as a potential risk or a threat and may lead to discriminatory ethnic profiling, which is by its nature difficult to reconcile with the obligation for national and EU law enforcement authorities and agencies not to discriminate on grounds of sensitive nature such as national or ethnic origin.

This section examines two sets of legal challenges affecting the nature and scope of EU JHA databases and the 'smart borders' initiative from a fundamental rights viewpoint. These large-scale IT systems stand in a sensitive relationship with Articles 7 and 8 (Private life and personal data), and Article 21 (non-discrimination) of the EU Charter of Fundamental Rights. The section's argument is that the European Commission's distinction between 'personal' and 'anonymous' data when categorising EU JHA databases is not fully conducive at times to understanding the legal aspects affecting these instruments. They not only raise questions from the perspective of protection of personal data of travellers. Independently from the personalised or anonymised nature of the data being collected and processed, they more generally have an impact on the general principles of EU law on privacy and non-discrimination, which lie at the foundations of the EU legal system.

First, this section will address the challenges of data protection and privacy (section 4.1). One of the challenges is the flexibility in the personal scope which leads to a blurring of 'who' is actually affected or targeted by these databases (i.e. EU citizens, third-country nationals with or without visa obligation, undocumented immigrants, asylum-seekers and refugees, etc.), and a high degree of legal uncertainty, weakening (even further) vulnerable data subjects, such as those holding an immigration administrative status. The right to privacy is equally affected by these systems, as well as the right to effective remedies. The compatibility of these systems with the principle of proportionality and other data protection tenets, such as purpose and time limitations, constitutes another open question to be considered when assessing the overall legality and necessity of EU JHA dataveillance systems.

Second, the challenge of discrimination will be examined (section 4.2). We will show that the logic of profiling and data-mining driving the rationale of JHA databases and 'smart borders', and their automated decision-making dimension based on 'statistical dataveillance', are in particular difficult to reconcile with the obligation for national and EU law enforcement authorities and agencies not to discriminate against individuals on grounds of a sensitive nature such as national or ethnic origin.

4.1 The challenges of data protection and privacy

The proliferation of data and information-exchange schemes in the context of EU JHA policies as well as the modification of existing ones as regards their size, scope and interoperability raise concerns related to the right to data protection and (more widely) to privacy of EU citizens and TCNs. One of our main arguments is that **independently from the personal character of the information collected and/or processed, large-scale IT systems are in tension with the general principle of privacy, which extends beyond data protection to the wider right to private life as envisaged in Article 7 of the EU Charter of Fundamental Rights**. This subsection focuses on specific challenges concerning the rights of data subjects (including information and effective remedies), necessity and proportionality and questions of purpose and time limitations. The questions raised here are the following: Who is targeted by these databases? Who is the physical incarnation of the personal data that is stored? What effective remedies are available? Instead of reviewing each fundamental principle of data protection,[124] this section will concentrate on the main challenges for large-scale databases in the EU.

[124] See the 9-point list suggested by Brouwer, Evelien: purpose limitation; transparency or purpose specification; extra safeguards for special categories of data; quality of data; individual participation or data subjects' rights; ban on automated decision-making; security; accountability and non-discrimination (in Brouwer, Evelien (2008), Digital Borders and Real Rights, *op. cit.*)

4.1.1 Who is targeted by JHA databases?

JHA databases have a very broad personal scope as they cover a wide range of individuals with a variety of legal statuses in accordance with EU law, as evidenced by the analytical table in Annex 1. The different categories of data subjects included, as well as the diversity of law enforcement actors having access to these data, create **a blurring of the individuals concerned by these EU systems.** As we addressed above, the EU RTP, which is originally foreseen to include only TCNs, might also cover certain EU nationals through the use of Automatic Border Control gates by some EU Member States.[125] From a legal perspective, the obscurity pertaining to the 'who' question has direct negative repercussions over **the principle of legal certainty**, according to which EU acts have to be clear and precise so as to allow those affected by them to determine without ambiguity their rights and obligations, and have access to the status and protection as data subjects.

The diversity characterising the personal scope of JHA Databases and smart systems fails to take into account that **certain travellers are more vulnerable than others**. This is for instance the case of undocumented immigrants and asylum seekers who are "minors, unaccompanied minors, disabled people, elderly people, pregnant women, single parents with minor children, victims of human trafficking, persons with mental disorders and persons who have been subjected to torture".[126] The storage of data concerning vulnerable travellers as 'data subjects' is especially relevant for the challenge of profiling and discrimination as addressed in the following subsection, and in particular in what concerns 'sensitive' data, which may be in fact more useful for the purposes of our study. The Council of Europe has defined sensitive data as "*personal data revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions, as well as other data defined as sensitive by domestic law.*"[127] The multiplication in the categories of targeted individuals, especially the vulnerable ones, is particularly problematic when it comes to ensuring effective remedies as we will also see below.

4.1.2 Anonymity and privacy

The uncertainty affecting the 'who' question has also direct repercussions over **the distinction between 'personal' and 'non-personal data'**, as underlined in section 2.1.3 above. Non-personal data has been said to include "*operational and strategic information*" which falls outside the scope of EU rules on the protection of personal data.[128] Non-personal data also covers "*de-personalised data*",[129] which can be defined as information about an individual that was anonymised, as well as "*dormant data*"[130] which present stricter rules of access.

---

[125] We have already addressed this issue in section 3.2.4.

[126] See Article 20(3) of European Parliament and Council of the EU (2011), Directive 2011/95/EU of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted (recast).

[127] See Council of Europe (2010), Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, CM/Rec(2010)13, 23 November 2010, point 1b.

[128] Recital 26 of the EU Data Protection Directive 95/46/EC reads: "*whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable*".

[129] See for example Frontex Regulation 1168/2011 (*op. cit.*), Article 11(3).

[130] See for example the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Council document 17434/11, 8 December 2011, Article 8.

Interestingly, neither the current EU data protection directive nor the proposals for a new regulation and a new directive[131] provide for commonly agreed technical definitions of these concepts of anonymous and dormant data, which can be particularly problematic in the area of law enforcement cooperation.

From a legal point of view, this distinction can be challenged by the fact that **personalised and anonymised data are both affected by the right to private life and the general principle of privacy.** It all comes back to the difference between data protection and privacy – the concept of privacy goes beyond the protection of personal data as it includes also non-personal elements that could influence private and family life. There is common agreement on the fact that

> the 'right to respect for private life' concerns a sphere within which everyone can freely pursue the development of his/her personality, which integrates the relations of individuals with other persons and with the outside world. Under this broad notion, the Strasbourg Court has included the protection of individuals against the processing of data related to them. In short, in EU law 'privacy' is (in principle) a broad notion that includes in its scope the protection of personal data, at least partially [...].[132]

Moreover, the distinction may become rapidly irrelevant in a context where JHA Databases rely on data-mining and the interlinking of classification factors. **The conditions under which de-personalised data can or could be re-personalised by law enforcement authorities** are therefore of utmost relevance when assessing this legal aspect. The definition of personal data thus depends on the capacity of law enforcement actors to personalise or to anonymise data. This issue of re-identification of anonymous data has been underlined by Council of Europe Recommendation CM/Rec(2010)13.[133]

These various dimensions of data and the discrepancies between divergent statuses of data are further enhanced by a lack of legal definitions regarding these aspects. This in turn can lead to legal uncertainties as regards the rights of data subjects, more specifically what individuals can do about their data, which will be addressed in the next sub-section.

4.1.3 Right and access to effective remedies

A wide range of categories of individuals are concerned by data processing in the framework of JHA Databases, from EU citizens to foreigners including vulnerable categories such as asylum seekers. Non-EU citizens can experience even more difficulties as regards **the right to be informed and to access their data and the right to challenge a decision and submit an appeal**.[134]

The right to be informed (or right of access) is a fundamental principle of data protection which enables data subjects to exercise control over personal data kept by third parties. It entails the possibility for any individual to be informed about the data storage and processing and to consult the stored information relating to her or him. As an example, Article 109 of the Schengen Convention concerning data stored in the SIS provides for the right of any person to

---

[131] See European Commission proposals COM(2012) 11 final and COM(2012) 10 final (op. cit.)

[132] See Bigo, Carrera et al (2011), Towards a New EU Legal Framework for Data Protection and Privacy, *op. cit.*, p. 20.

[133] See Council of Europe (2010), Recommendation CM/Rec(2010)13 (*op. cit.*) point 8.5: "Suitable measures should be introduced to guard against any possibility that the anonymous and aggregated statistical results used in profiling may result in the re-identification of the data subjects."

[134] See Carrera, De Somer and Petkova (2012), The Court of Justice of the European Union as a Fundamental Rights Tribunal, CEPS Liberty and Security Paper No49, August 2012, p. 5.

have access to data relating to him.[135] At a border zone however, the practicality of informing a TCN about his/her rights as a data subject and about accessibility to remedies against refusal of entry remains unclear.[136] In the context of JHA databases, this raises the question of how to ensure that an individual becomes a 'data subject' enjoying the full arsenal of his/her rights.

The right to effective remedies constitutes another general principle of EU law. General principles have been developed by the CJEU and constitute unwritten rules not expressly provided for in the treaties but which affect how EU law is interpreted and applies. They stem from public international law, common constitutional principles from EU Member States and human rights. The right to effective remedies has been enshrined by the CJEU as a general principle of EU law in 1986 in the *Johnston* case.[137] Furthermore, Article 47 of the EU Charter of Fundamental Rights guarantees the right to an effective remedy and to a fair trial to 'everyone'. **The question of effective remedies becomes central in the case of non-EU citizens whose names and personal information may be stored in an EU database**. Individuals from third countries face more vulnerabilities and barriers at times of exercising their right to seek justice in front of the database manager or before a court regarding the content and use of stored information, as they encounter difficulties in getting information and having access to remedies both when they are in an EU member state and when they are outside EU territory.

A well-known example concerns the Moon affair, where the Korean leader of the Unification Church was prevented to enter German territory due to his name being listed in the SIS database in 1995. German authorities refused to grant him access to the German territory for reasons of public security due to Mr Moon's church being considered as a religious cult. This case is interesting due to the fact that it took 12 years for German courts to rule on his case, which challenges the assumption of 'effective' remedy in the case of the SIS:

> The current use of the SIS for immigration law purposes has already established that it is extremely difficult for individuals and their lawyers to remedy a false or unlawful SIS report. The Commission's proposals for further "automated decision making at the borders" will undoubtedly increase the problems of individuals seeking legal redress against negative decisions.[138]

The existence of various EU systems and databases for exchange of information between EU and national law enforcement authorities increase the possibilities for personal data to be processed by different authorities in different Member States and working on different policy areas. This multiplication of legal orders complicates the access for individuals to their right to an effective remedy. As a possible solution to this problem, the EDPS has very often in the past advocated for, on one hand, the establishment of common EU standards on data subjects' rights as regards JHA databases, and on the other hand, the possibility for individuals to have access to

---

[135] See Convention of 19 June 1990 applying the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at their Common Borders, OJ 2000 L 239, 1990, articles 109 and 110.

[136] The right to be informed is envisaged in Article 13.2 and right of appeal in Article 13.3 of the Schengen Borders Code (Regulation (EC) No 562/2006, *op. cit.*). There is no obligation to inform the TCN in a language he/she can understand.

[137] Court of Justice of the European Union (1986), Case 222/84 Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary, 15 May 1986, ECR 1651.

[138] Brouwer, Evelien (2008), The Other Side of Moon - The Schengen Information System and Human Rights: A Task for National Courts, CEPS Working Document No. 288/April 2008, p. 16.

effective remedy in front of both authorities that make data available and that access and process these data.[139]

4.1.4 Are JHA databases necessary?

The question of the 'who' brings us to the logical question of the 'what and why' – which kind of data is stored in these databases and why? Is the collection, storage and processing of data related to borders and crime necessary? **This legal challenge is embodied in the necessity debate surrounding the establishment of JHA databases, which lies at the heart of the proportionality principle testing.** As data protection and privacy are fundamental human rights enshrined in the Charter as well as in the European Convention on Human Rights, any interference with these rights and principles must be duly justified on the side of the interferer. Article 8(2) ECHR underlines the fact that the interference should be "*in accordance with the law and [...] necessary in a democratic society*".

The review of the necessity and proportionality of a measure affecting privacy has been widely discussed by the European Court of Human Rights in its case-law.[140] In the *Marper v United Kingdom* case, the Court addressed the wording "*in accordance with the law*" in the context of storage of personal data, linking it to the rule of law. It was held that data collection and processing needs to have a "*legitimate purpose*" whereas the retention of data is required to be "*proportionate*" in relation to this legitimate purpose.[141]

The CJEU in turn also addressed the question of necessity in the *Huber v Germany* case in 2008, which concerned reviewing the legality of a centralised database in Germany holding information on non-German EU citizens for ensuring the compliance with the conditions of residence and the fight against crime (Gonzalez et al., 2010).[142] Some of the points made by the CJEU are of particular relevance for the purposes of this study, especially as regards the limitation of access to personal data to authorities having powers in that field only, or on the fact that statistical tools only require anonymous data and not personal data.[143] Prior to the judgment, the Advocate-General Maduro had arrived at the same conclusions, underlining the question of effectiveness ("It is not necessary for the alternative system to be the *most* effective or appropriate; it is enough for it to be able to perform adequately") and highlighting that the necessity test required "a pressing social need".[144]

The mapping of existing and future databases provided in Annex 1 of this study demonstrates that most of the JHA databases serve the purpose of fighting crime and controlling the external borders, which are automatically assumed to be necessary purposes in a democratic society. However, this assumption is more and more challenged even on the side of EU decision-makers,

---

[139] See among others European Data Protection Supervisor (2006), Opinion of 28 February 2006 (*op. cit.*).

[140] See European Court of Human Rights (1976), Case Handyside v The United Kingdom, 7 December 1976, 1 EHRR 737, where the Court further specified proportionality and necessity with a four-questions test: Is there a pressing social need for some restriction of the Convention? If so, does the particular restriction correspond to this need? If so, is it a proportionate response to that need? In any case, are the reasons presented by the authorities, relevant and sufficient?

[141] See European Court of Human Rights (2008), *S and Marper v United Kingdom*, op. cit., notably points 95, 100 and 107.

[142] Gonzalez Fuster, de Hert, Ellyne and Gutwirth (2010), Huber, Marper and Others: Throwing New Light on the Shadows of Suspicion, CEPS INEX Policy Brief, Brussels, 2010.

[143] See Court of Justice of the European Union (2008), Case C-524/06 Heinz Huber v Bundesrepublik Deutschland, 16 December 2008, notably points 61 and 65.

[144] See Opinion of Advocate General Poiares Maduro on Case C‑524/06 "Heinz Huber v Bundesrepublik Deutschland", 3 April 2008, points 16 and 27.

as seen above in section 3.1.2 with the example of the Polish Presidency harbouring doubts in 2011 about the necessity and effectiveness of the 'smart borders' legislative proposal.[145] The EDPS has also critically challenged the necessity and proportionality of this proposal, mainly on the basis of a lack of reliable evidence to support the need of new systems.[146] The EDPS also underlined the lack of evaluation of existing systems, the interoperability between databases as well as the generalisation of surveillance and the risks to the presumption of innocence as the main challenges of the smart borders proposal.

4.1.5 (Un)purpose and timeless limitations

A further specific challenge for the use of EU databases by public authorities concerns another key principle of data protection in the European legal system, i.e. the principle of purpose limitation and, by extension, the dilemma of 'purpose un-limitation' inherent to JHA Databases and smart borders initiatives. This principle provides that **personal data must be collected for specified, explicit and legitimate purposes and must not be further used in a way incompatible with those purposes**.[147] Purpose limitation is often seen by EU decision-makers as 'soft law', i.e. a guideline that should be followed only if necessary. However, purpose limitation is a legal principle enshrined in Article 6(1)(b) of the EU Data Protection Directive[148] as well as Article 5(b) of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[149]

The case-law of the CJEU and of the European Court of Human Rights have further reinforced the meaning and importance of purpose limitation: in the case Kruslin v. France,[150] a telephone tapping ordered by an investigating judge in a murder case led to a violation of Article 8 ECHR because the law did not indicate with sufficient clarity the scope and manner of data collection by French authorities. Similarly, the case Rotaru v. Romania[151] concerning a law on data collection in secret files that did not specify which information could be stored, and against which categories of people or under which circumstances these surveillance measures were allowed, led to a condemnation of Romania by the Strasbourg Court.

The CJEU also clarified the notion of purpose limitation in the *Huber* case, already mentioned above.[152] In this case, the Court had to assess the legitimacy of three different purposes of the German central aliens database (AZR): first, the use for administrative purposes by border

---

[145] Polish Presidency of the European Union (2011), Sopot Conclusions (*op. cit.*)

[146] European Data Protection Supervisor (2008), Preliminary Comments on the proposed border package, 3 March 2008, p. 3.

[147] Brouwer, Evelien (2011), Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation, in Leonard Besselink, Frans Pennings & Sacha Prechal (eds), The Eclipse of the Legality Principle in the European Union, Kluwer Law International, p. 273.

[148] Directive 95/46/EC (*op. cit.*), article 6(1)(b) states that "Member States shall provide that personal data must be [...] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".

[149] Council of Europe (1981), Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981. Article 5(b) states that "Personal data undergoing automatic processing shall be [...] stored for specified and legitimate purposes and not used in a way incompatible with those purposes."

[150] European Court of Human Rights (1990), Kruslin v. France, judgment of 24 April 1990, Series A no.176-A, and Huvig v. France, judgment of 24 April 1990, Series A no.176-B.

[151] European Court of Human Rights (2000), Rotaru v. Romania, judgment of 4 May 2000, application no. 28341/95

[152] See Court of Justice of the EU (2008), Huber case C-524/06 of 2008 (*op. cit*).

control authorities; second, the use of the AZR for statistical purposes; and third, the use of the data on EU citizens for law enforcement purposes. Interestingly, in this judgment, the Court made a link between purpose limitation and non-discrimination, which will be addressed in Section 4.2.

In the context of data processing in large-scale databases, the notion of purpose limitation is central for gaining a better understanding and limiting the 'function creep' that new technological law enforcement systems inevitably bring along with them. The notion of **function creep can be seen as a virtual line between a lawful and justified data processing system and a surveillance tool** – crossing that line entails going away from the original purpose of the system. In the case of JHA databases, three developments can be seen as paradigmatic of the erosion of the principle of purpose limitation: the Commission's proposal on interoperability of different EU databases, launched in 2004 but abandoned due to a lack of support by Member States;[153] the possibility for Europol and other law enforcement authorities to have access to the Visa Information System[154] and even to Eurodac[155]; and the collection and exchange of DNA profiles between Member States under the Prüm Decisions.[156]

Interoperability between various databases challenges the purpose limitation because personal data previously available for specific purposes only might be accessed for different purposes than originally legislated upon. The same line of reasoning goes for the VIS and Eurodac being accessible by Europol and other law enforcement authorities, deviating the original purpose from visa and asylum management to the fight against crime (which, in the case of Eurodac, implies that asylum seekers are to be treated as suspected criminals).[157] In the case of Prüm, safeguards include the anonymity of DNA samples and the hit/no hit approach used for DNA comparisons under the Prüm Decisions, which provides law enforcement agents with access to reference data only, and not personal data. However, once DNA data and related information are available, the possibility of function creep undoubtedly remains present.[158]

A corollary to the question of purpose limitation is time limitation. How long should the data be stored? What happens to personal data after the time limit has expired? Legal instruments only specify that personal data should be kept "for no longer than is required for the

---

[153] European Commission (2005), Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490, 12 October 2005.

[154] Council of the EU (2008), Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences OJ L 218/129, 13 August 2008.

[155] European Commission (2009), Amended proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints, COM(2009) 342 final, 10 September 2009

[156] Council of the EU (2008), Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council of the EU (2008), Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[157] See for example the Meijers Committee expressing concerns about Eurodac being accessible by law enforcement authorities (last accessed 10/11/2012): www.commissie-meijers.nl/assets/commissiemeijers/CM1216%20Note%20Meijers%20Committee%20on%20the%20EURODAC%20proposal.pdf?

[158] For recent debates about the Prüm decisions, see Hernanz, Nicholas (2012), More Surveillance, More Security? The Landscape of Surveillance in Europe and Challenges to Data Protection and Privacy – Policy Report on the Proceedings of a Conference at the European Parliament, SAPIENT Deliverable 6.4, January 2012

purpose for which those data are stored".[159] The question of time limits reveals a lack of common standards in the context of JHA databases, especially in the case of Passenger Name Records (PNR).[160]

As we addressed in section 2.1.4 of this note, the point of convergence of the trends characterising the establishment and use of JHA databases is clearly a move towards multi-functional, multi-actor and multi-purpose schemes. **This creates legal uncertainties as the thin line between different policy areas is crossed when processing data related to borders, crime or fight against terrorism.**

4.2 The challenge of discrimination

A key systemic issue inherent to EU databases and smart borders relates to their implications over the principle of non-discrimination. They raise important questions of non-discriminatory treatment which constitutes a general principle of EU law and are covered by specific package of European secondary legislation, now enshrined as a fundamental human right in Article 21 of the EU Charter of Fundamental Rights. There are two main factors of particular importance when assessing the discrimination-related legal challenges emerging from JHA Databases: First, the logics of profiling and data-mining driving their scope and reach; and second, the legal status of the individuals covered or targeted by these systems (citizens / foreigners).

4.2.1 Legal status and non-discrimination: citizens and foreigners

There is an ample group of people who are and will be covered by EU JHA databases and the 'smart' dataveillance initiatives. Their personal scope extends beyond those labelled as TCNs to cover also individuals holding the nationality of an EU Member State, i.e. EU citizens. Some of these systems apply also to EU nationals (e.g. PNR, TFTP, VIS, etc). This goes along with an open-ended (flexible) nature of 'who is targeted' (or to be targeted) by these technologies (e.g. RTPs, where EU citizens may be also included in a later stage). The legal categorisation within which the individual falls into is of utmost relevance at times of identifying the applicable law and the degree of non-discrimination protection granted.

The body of legislation at EU level ensuring equality of treatment has traditionally covered individuals holding the nationality of an EU Member State (EU citizens) in accordance with Article 20 of the Treaty on the Functioning of the European Union (TFEU). Non-discrimination in European law has largely focused on EU citizens when exercising their right to freedom of movement and residence (free movement of persons) in a second EU Member State and while doing so not been discriminated on the basis of nationality in comparison to nationals of the receiving country (Article 18 TFEU). The CJEU confirmed this principle in its above-mentioned landmark judgement *Huber* C-524/06. The CJEU concluded that the database in question and the systematic processing of personal data was incompatible with EU citizenship and free movement legislation as it only covered non-German EU citizens for crime-fighting purposes. The justification provided by the German government to "*protect the public order*"

---

[159] Council of Europe (1981), Convention 108 (*op. cit.*), article 5(e). Article 6(1)(e) of EU Directive 95/46/EC is very similar.

[160] For example, the EU-Canada PNR agreement provides for a regular storage time of 3.5 years and exceptionally a maximum of 6 years. The EU-Australia PNR agreement provides for a maximum retention time of 5.5 years. In the EU-United States PNR agreement, the regular storage time is of 10 years for crime, 15 years for terrorist offences. The EU's own PNR proposal, finally, considers 5 years maximum retention as appropriate. This argument was already presented in Geyer, Florian (2008), Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice, CEPS Liberty and Security Research Paper No 9, May 2008.

was not accepted as sufficient by the Court to justify the necessity of the database, and declared that difference in treatment between those nationals and those Union citizens was discriminatory in nature and therefore incompatible with Article 18 TFEU.[161]

Third country nationals (TCNs) are in principle not covered by the protection conferred by EU anti-discrimination law on grounds of nationality and legal status. Nationality is not part of the prohibited grounds of discrimination in the EU legal system as outlined in Article 19 TFEU, which resides now under the heading 'Non-discrimination and citizenship of the Union'. It is precisely on the basis of the acceptance of the citizen-foreign divide, and discrimination on the basis of nationality in the conditions of entry, that borders controls find their rationale and official legitimisation. Yet, as Schiek, Waddington and Bell (2007) have rightly argued, nationality poses a particularly challenging question to EU non-discrimination legislation.[162] This is particularly relevant as regards the extent to which protection applies to TCNs already present in the EU and whether they have a right to claim that protection in what concerns conditions of residence. The grounds upon which this protection may be claimed are of key importance in this respect.

Non-discrimination legislation at EU level has been built upon a list of prohibited grounds beyond nationality, which correspond with: racial and ethnic origin, religion and belief, sexual orientation, disability and age, gender (Bell, 2008 and 2002).[163] These are currently envisaged in a package of legislative secondary law measures, i.e. the Employment Equality Directive,[164] the Race Equality Directive[165] and the various Gender Equality Directives.[166] Both the Race and the Employment Equality Directives state the prohibition of discrimination applies also to TCNs. However, it is also true that they do not equate the treatment granted to EU citizens to TCNs in what concerns the legal conditions of entry and residence. Specifically, the Race Directive 2000/43 prohibits discrimination on the basis of race and ethnic origin. No definition is provided by the act about the actual meaning and scope of this category. One of the more consensual concepts can be found in the International Convention on the Elimination of All Forms of Racial Discrimination, which states in its Article 1 that racial discrimination means

> …any distinction, exclusion, restriction or preference based on *race, colour, descent, or national or ethnic origin* which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise on an equal footing, of human rights and

---

[161] Court of Justice of the European Union (2008), *Heinz Huber, op. cit.*. The Court held that

> …principle of non-discrimination… requires that comparable situations must not be treated differently and that different situations must not be treated in the same way. Such treatment may be justified only if it is based on objective considerations independent of the nationality of the persons concerned and is proportionate to the objective being legitimately pursued.

[162] Schiek, D., Waddington, L. and Bell, M. (eds) (2007), *Cases, Materials and Text on National, Supranational and international Non-Discrimination Law*, Portland, Oregon: Hart Publishing.

[163] Bell, M. (2008), "The Implementation of European Anti-Discrimination Directives: Converging towards a Common Model?", *The Political Quarterly*, Vol. 79, No. 1, 2008, pp. 36-44. See also Bell, M. (2002), *Anti-Discrimination Law and the European Union*, Oxford: Oxford University Press.

[164] Council of the EU (2000), Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation

[165] Council of the EU (2000), Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, hereafter "Race Directive" OJ L180, 19/07/2000, p. 22–26.

[166] European Parliament and Council of the EU (2006), Directive 2006/54/EC of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast)

> fundamental freedoms in the political, economic, social, cultural or any other field of public law.[167] (Emphasis added).

The body of the 2000/43 Directive is clear at times of stating that its material scope excludes differential treatment on the basis of nationality and is "*without prejudice to provisions and conditions relating to the entry into and residence of third country nationals…and to any treatment which arises from the legal status of the third country nationals"* (Article 3.2). However, the Preamble confirms its application to TCNs when saying:

> (13) To this end, any direct or indirect discrimination based on racial or ethnic origin as regards the areas covered by this Directive should be prohibited throughout the Community. *This prohibition of discrimination should also apply to nationals of third countries*, but does not cover differences of treatment based on nationality and is without prejudice to provisions governing the entry and residence of third-country nationals and their access to employment and to occupation. (Emphasis added)

Other pieces of EU migration and border law include non-discrimination related clauses as regards conditions of entry and residence of TCNs. Illustrative examples are the Long-Term Residents TCNs Directive 2003/109,[168] or the Schengen Borders Code (SBC),[169] which stipulates in Article 6.2 (the conduct of border checks) that "*While carrying out border checks, border guards shall not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation*." Therefore, **while nationality and legal status may not be considered as connecting factors for activating the EU non-discrimination system of protection for TCNs, any persons (independently of their migration administrative status) are nonetheless beneficiaries of the general non-discrimination protection on the basis of racial or ethnic origin, religion or belief, sex, disability, age or sexual orientation.** Non-discrimination is after all a well-established legal principle in the EU legal regime which is formally stipulated in a wide range of international and European legal human rights legal instruments (most notably in the framework of the United Nations and the Council of Europe) to which all EU member states are party, and which is now expressly enshrined in Article 21 of the EU Charter (Wiesbrock, 2010).[170] These apply equally to EU citizens and foreigners (Guild, 2004).[171]

That notwithstanding, there are however important **difficulties at times of ascertaining the applicability and effective delivery of the non-discrimination protection to TCNs**. Their vulnerable status plays here also a role. **It is too often challenging to distinguish discrimination on the basis of race and ethnic origin, from that of 'nationality',** which to a large extent depends on the conceptual bases which are taken; is it a legal status? Or is it a wider status which may be ascribed to ethnicity and/or origin? The boundaries between ethnic origin

---

[167] The term 'race' has been subject to wide criticism, as it presumes that persons can be differentiated according to 'races'. The Race Directive takes position on this point by saying that "(6) The European Union rejects theories which attempt to determine the existence of separate human races. The use of the term "racial origin" in this Directive does not imply an acceptance of such theories." Instead, other categories such as origin or ethnicity have been preferred by the literature.

[168] (5) Member States should give effect to the provisions of this Directive without discrimination on the basis of sex, race, colour, ethnic or social origin, genetic characteristics, language, religion or beliefs, political or other opinions, membership of a national minority, fortune, birth, disabilities, age or sexual orientation.

[169] Schengen Borders Code, *op. cit.*

[170] Wiesbrock, A. (2010), *Legal Migration to the European Union: Ten Years After Tampere*, Martinus Nijhoff Publishers.

[171] See Guild, Elspeth (2004), "The Variable Subject of the EU Constitution, Civil Liberties and Human Rights", European Journal of Migration and Law, Vol. 6, No. 4, 2004.

and national origin, or between national origin and nationality, are indeed difficult to capture in practice (Brown, 2002).[172] Schiek et al have expressed the view according to which "*In many cases, discrimination against non-nationals and discrimination based on national and ethnic origin will coincide, especially since there is a considerable overlap between minority ethnic communities in Europe and communities of third country nationals. In some cases, 'nationality' thus seems to be used not so much to refer to someone's legal nationality, as to someone's country of birth or ethnic background*" (Schiek, Waddington and Bell, 2007, p. 65).

Therefore, **the exclusion of nationality discrimination in the scope of the Race Equality Directive is somehow at odds with a reality where discrimination of TCNs is multi-ground or multi-faceted, where questions of ethnicity, legal status, nationality, religion, etc might be too often intertwined and difficult to disentangle from one another.** How can border controls be carried out in such a way that they discriminate only on grounds of nationality and in a way by which nationality does not become a proxy ground for those which are otherwise prohibited? Do some border control actors use nationality discrimination as a formally permitted ground of discrimination but which in fact is used to justify indirect discrimination on prohibited grounds?

The same difficulty applies when trying to dissociate discrimination on the basis of nationality and/or ethnic origin in the scope of profiling and data-mining practices logics driving JHA Databases and Smart Borders systems. **The statistical dataveillance subsumed in their scope and working arrangements relies on 'discrimination by default'.** Questions at stake in this discussion include for example: What are the factors determining that a particular individual meets the profile or risk category in the EU system? Which kinds of data, characteristics or grounds are used in the statistical categorisation of individuals? Which law enforcement authorities will have access to these data and for which purposes? The answers to these same questions will ultimately determine the lawfulness of the EU data and information exchange schemes with EU non-discrimination legislation. From the analysis conducted in this study, one is inclined to think that JHA Databases and Smart Borders may easily engage into what ECRI has called 'racial profiling', i.e.

> The use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or national or ethnic origin in control, surveillance or investigation activities.[173]

Moreover, as the United Nations Human Rights Committee held in the 2009 *Rosalind Williams Lecraft v Spain* case, which dealt with race and ethnicity motivated identity checks by the police, while it is legitimate for law enforcement authorities to carry out checks for reasons of public safety and security or with a view to controlling irregular immigration, however,

> … when the authorities perform such controls, ***the mere physical or ethnic features*** **of the persons subject to them should not be taken as indicative of their possible illegal status in the country. Neither should such checks be made such that only persons with given physical or ethnic features are selected**. Doing otherwise would not only adversely affect the dignity of the persons affected, but would also contribute

[172] Brown, C. (2002), The Race Directive: Towards Equality for All the Peoples of Europe?, *YEL* 210.

[173] European Commission against Racism and Intolerance (ECRI) (2007), ECRI General Policy Recommendation No. 11, on combating Racism and Racial Discrimination in Policing, CRI(2007)39, 29 June 2007.

> to spreading xenophobic attitudes among the population at large and would be inconsistent with an effective racial discrimination prevention policy.[174]

The logics of profiling and data-mining driving the rationale of JHA Databases and Smart Borders, and the potential use of race, ethnicity, religion or other sensitive grounds as the main or sole basis of classification and statistical dataveillance activities of TCNs and EU citizens are therefore incompatible with non-discrimination legal obligations stemming from EU and international law and are henceforth unlawful.

4.2.2 Statistical surveillance and statistical discrimination

JHA Databases and smart borders work on the basis of **'automated decision making'** parameters, which correspond with what has been denominated as **'profiling' or 'predictive data-mining' in the EU security field** (Hildebrandt and Gutwirth, 2008). The Council of Europe (CoE) has defined 'profiling' as "*an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*."[175] The CoE also signalled the profiling technique may be capable of having an impact on the people concerned by placing them in 'predetermined categories', even if the profile remains anonymous in nature. In a 2009 recommendation, the European Parliament highlighted that:

> ...profiling, whether through data-mining or the practices of police and other agencies, is increasingly used as a tool for law enforcement and border control, and insufficient regard is being given to the evaluation of its effectiveness and to the development and application of legal safeguards to ensure respect for rights of privacy and the avoidance of discrimination.[176]

The data collected is processed by calculation and statistical correlation with the aim of producing risk profiles. Profiling has been therefore highly controversial because it produces **probabilistic knowledge**: statistics showing that a particular group of individuals has a higher chance of being involved in a criminal or unlawful activity will justify that profilers focus their efforts on that particular group. In the field of law enforcement more concretely, **profiling is used 'to select' a group of people as a potential risk or a threat – such as 'high risk travellers', 'suspicious traveller', the visa 'over-stayer', etc, which may lead to discriminatory ethnic profiling** (FRA, 2010).[177] The objective is to prevent crime based on selective data-mining identifying people that are deemed to deserve closer attention by tracing some of their current characteristics' at times of foreseeing their potential future behaviour (Fuster, Gutwirth and Ellyne, 2010). This practice is what Gandy has called **'statistical surveillance'** in the governance of mobility, which refers to these kind of statistical techniques/technologies of control as "*classificatory systems as technologies of discrimination*".[178] Gandy understands '*statistical discrimination*' as "a *decision to exclude or deny opportunity to an individual on the basis of the attributes of the group to which he or she is*

---

[174] Court of Justice of the European Union (2009), *Rosalind Williams Lecraft v Spain,* Comm No. 1493/2006, 30 July 2009, para. 7.2.

[175] Council of Europe (2010), Recommendation COM/Rec(2010)13, *op. cit.*

[176] European Parliament (2008), Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)), Rapporteur Sarah Ludford, pt. E.

[177] European Union Agency for Fundamental Rights (FRA) (2010), Towards More Effective Policing – Understanding and Preventing Discriminatory Ethnic Profiling: A Guide, Vienna, 2010.

[178] Gandy, O. H. Jr (2012), Statistical Surveillance: Remote Sensing in the Digital Age, in Ball, Haggerty and Lyon (eds.), Routledge Handbook of Surveillance Studies, Routledge.

assumed to belong….as a result, what would otherwise be treated as illegal racial discrimination is routinely justified as a legitimate and inherently rational act".[179]

In the context of the EU databases examined in this study, and as demonstrated by the Sections developed above, the EU is putting more efforts into 'profiling' without actually expressly acknowledging that practice and duly assessing the legal aspects underlying statistical dataveillance. **The logics of profiling and data-mining pertaining to EU JHA Databases and Smart Borders are by nature difficult to reconcile with the obligation for national and EU law enforcement authorities and agencies not to discriminate on grounds of sensitive nature such as national or ethnic origin.** The next subsection argues that from an EU law point of view JHA Databases open up concerns from a non-discrimination perspective in what concerns both TCNs (non EU nationals) and EU citizens moving.

[179] Gandy, O. H. Jr (2009), Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage, Burlington, VT: Ashgate, pp. 69-72.

5. Recommendations

Given the state of existing knowledge on the JHA landscape of data and information schemes, **the question of monitoring and oversight by the European Parliament, and jointly with national parliaments, is central**. In this respect, we offer the following recommendations:

1. The European Parliament should require the European Commission **to provide on a regular basis, possibly yearly, a consolidated monitoring report of the activity of all schemes involving data and information exchange in the JHA policy domain**. The report should include statistics on the records created, held and/or exchanged by means of these schemes, as well as details of activities such as access (**by country/authority**). Blueprints for such a report include the Commission's own 2010 communication as well as the reports of activity of EUROPOL and EUROJUST and their Joint Supervisory Bodies.

2. The European Parliament **should work towards the establishment of an oversight mechanism involving national Parliaments providing a yearly, detailed listing of all the persons who have had access, in the context of EU-related measures, to data and information exchange schemes**. This listing would account for the number of accesses per person, per file within a given database, per database and across databases (accounting for availability and interoperability provisions).

3. These systems of monitoring and oversight **would lead to the constitution of an evidence base to assess the effective reliance of law-enforcement services on EU related data and information schemes in the field of JHA**. This evidence base should be used to decide upon the continuation of existing schemes (reversibility) as well as the adoption of new schemes (necessity, originality).

4. **Any further development incurring costs to the EU budget should be halted until work towards the establishment of these two mechanisms has sufficiently advanced**. This includes the 'smart borders' initiatives as well as EU-PNR, EU-TFTS and EUROSUR, as well as any other possible forthcoming proposal.

There is a clear need **to examine further the assumptions on which the 'smart borders' initiative is based**, from the point of view of necessity and originality, as well as costs. In this regard, we offer the following recommendations:

5. **The European Parliament should sponsor an in-depth, independent evaluation of already existing Entry/Exit Systems and registered traveller programmes** running at national level among Member States and in key third countries, including the United States and Australia. This assessment would be **coordinated by the Science and Technology Options Assessment unit** (STOA). Without prejudice to the final decision of the STOA panel, such an assessment exercise would involve technologists, data protection experts, lawyers specialised in the right to privacy and non-discrimination, as well as social science researchers (political science, sociology and international relations specialists) with a record of investigation in law-enforcement activities. Civil society organisations should also be allowed an input into the workings of this expert group.

6. Regarding costs, the European Parliament should issue **a request to the European Court of Auditors to conduct, as laid out in Article 287 TFEU, an inquiry into the implementation of EU security research and External Border Fund** with regard to 'smart borders' and EUROSUR. The negotiation on a 'smart borders' legislative instrument should be conditional on the outcome of this inquiry, and take into account the amounts already earmarked and spent on this initiative.

7. Within the context of possible negotiations on measures related to the establishment of additional data and information schemes in the area of external border control, the European Parliament should **seek clarification of the exact relationship between any future EES and VIS and SIS/SIS II if this is not clearly defined in the future draft legislative proposal**. The European Parliament should seek to **extend the provisions in the draft EUROSUR Regulation on financial accountabilit**y to require FRONTEX and the European Commission to provide **an annual report detailing all expenditure on EUROSUR-related developments from all EU budget lines, including the External Borders Fund, proposed Internal Security Fund, FP7 and Horizon 2020 and the Development Cooperation Instrument**.

8. The logics of profiling (automated decision making) and data-mining characterizing JHA Databases and Smart Borders, and the potential use of race, ethnicity or other sensitive grounds as basis of statistical dataveillance are difficult to reconcile with non-discrimination principles, secondary legislation and fundamental rights obligations. Existing and forthcoming JHA Database should foresee **non-discrimination by default**, which should be closely linked with ensuring data protection principles (right of information, effective remedies and individual consent for data processing) to TCNs, with particular attention to vulnerable categories of TCNs as data subjects. Particular attention should be paid to **strictly limiting 'scope, law enforcement actor access and purpose creep'** in their rationale, functionalities, and intended public goal.

9. The Smart Borders initiatives must go hand-to-hand with the provision of **a definition of profiling** in the newly proposed EU legal framework on data protection in the field of law enforcement, currently under negotiations. This definition should include the kind of profiling practices that should be always prohibited and solid legal safeguards for those that are considered to be legitimate. The statistical discrimination logic driving JHA Databases and 'smart' systems needs expressly to adhere to the general data protection principles.

10. JHA Databases and Smart borders pose profound legal challenges from the perspectives of proportionality and legal certainty. Besides the costs assessment mentioned above, the European Parliament should carry out **its own (independent) impact assessment** of the upcoming Commission legislative proposals covering the EES and the RTP. Particular attention should be there paid to the necessity, suitability and wider societal implications inherent to the development of these large-scale information systems.

In the perspective of the adoption of the EU's 2014-2020 Multiannual Financial Framework, the European Parliament should consider the following:

11. The **Internal Security Fund should be implemented according to the 'partnership principle'**, with relevant civil society organizations and international NGOs regularly consulted on the impact and added value of the initiatives funded at national and EU level and their effect with regard to fundamental rights and non-discrimination. **At a minimum, this principle must apply to the mid-term review of the ISF in 2017 and the evaluation of member state programmes**.

12. The **draft Horizon 2020 legislation should be amended to provide for European Parliamentary control over the annual Calls for Proposals**. In the area of security and space research this process should ensure that **calls for EU-funded research address fundamental rights concerns from the outset, meet a verifiable security need and provide value for money**.

13. A central priority should be gaining **a full picture of the financial repercussions** (across the various EU funding schemes) involved in their establishment and development at EU,

national and regional/local levels. The European Parliament should be involved (have a binding say) in the framing of the policy priorities agreed between the Commission and the Member States - **the Policy Dialogue** - in the context of multiannual programmes in order to ensure that those national programmes and projects funded correspond fully with EU policy priorities. Also, the European Parliament should be involved in the policy priorities determined by DG Home in the context of Union Actions, which are in exclusive hands of the Commission.

References

Literature

Bell, M. (2002), Anti-Discrimination Law and the European Union, Oxford: Oxford University Press.

———— (2008), "The Implementation of European Anti-Discrimination Directives: Converging towards a Common Model?", The Political Quarterly, Vol. 79, No. 1, 2008, pp. 36-44.

Bigo, Carrera et al (2011), Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament, Study for the European Parliament, PE 453.216, CEPS, Brussels, September 2011

Bigo, Didier, Jeandesboz, Julien (2008), Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research, PE 393.289, Brussels.

Brouwer, Evelien (2008), Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System, Leiden: Martijnus Nijhoff.

———— (2008), The Other Side of Moon: The Schengen Information System and Human Rights: A Task for National Courts, CEPS Working Document No. 288, CEPS, Brussels, April 2008.

———— (2011), Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation, in Leonard Besselink, Frans Pennings & Sacha Prechal (eds), The Eclipse of the Legality Principle in the European Union, Kluwer Law International.

Brown, C. (2002), The Race Directive: Towards Equality for All the Peoples of Europe?, YEL 210.

Bruggeman, Willy (2006), What are the options for improving democratic control of Europol and for providing it with adequate operational capabilities, PE 378.274, Brussels.

Burgess, J. P., Hanssen, M. (2008), Public Private Dialogue in Security Research, PE 393.286, Brussels.

Carrera, De Somer and Petkova (2012), The Court of Justice of the European Union as a Fundamental Rights Tribunal, CEPS Liberty and Security Paper No49, August 2012.

De Hert, Bellanova (2009), Data Protection in the Area of Freedom, Security and Justice: A System to Be Fully Developed?, PE 410.692, March 2009.

Drewer, Ellerman (2012), Europol's data protection framework as an asset in the fight against cybercrime, ERA Forum, Volume 13, Issue 3, November 2012, pp 381-395.

Fortmann, M., Roussel, S., Macleod, A. eds (2003), Vers des périmètres de sécurité? La gestion des espaces continentaux en Amérique du Nord et en Europe, Montreal: Athena.

Gandy, O. H. Jr (2009), Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage, Burlington, VT: Ashgate, pp. 69-72.

———— (2012), Statistical Surveillance: Remote Sensing in the Digital Age, in Ball, Haggerty and Lyon (eds.), Routledge Handbook of Surveillance Studies, Routledge.

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

Gonzalez Fuster, de Hert, Ellyne and Gutwirth (2010), Huber, Marper and Others: Throwing New Light on the Shadows of Suspicion, CEPS INEX Policy Brief, Brussels

Guild, Elspeth (2004), "The Variable Subject of the EU Constitution, Civil Liberties and Human Rights", European Journal of Migration and Law, Vol. 6, No. 4.

Hayes, Ben, Vermeulen, Mathias (2012), Borderline: The EU's New Border Surveillance Initiatives, Berlin: Heinrich Böll Foundation.

Hempel, Carius et al (2009), Exchange of information and data between law enforcement authorities within the European Union, Study for the European Parliament, PE 419.590, CEPS, Brussels, April 2009

Hernanz, Nicholas (2012), More Surveillance, More Security? The Landscape of Surveillance in Europe and Challenges to Data Protection and Privacy – Policy Report on the Proceedings of a Conference at the European Parliament, SAPIENT Deliverable 6.4, January 2012.

Hobbing, Peter (2006), An Analysis of the Commission Communication (COM(2005) 597 final) of 24.11.2005 on Improved Effectiveness, Enhanced Interoperability and Synergies among European Databases in the Area of Justice and Home Affairs – Briefing Paper for the European Parliament, PE 378.270, Brussels, February 2006.

Hobbing, Peter, Kowslowski, Rey (2009), The tools called to support the 'delivery' of freedom, security and justice: a comparison of border security systems in the EU and in the US, PE 410.681, Brussels, February 2009.

Jeandesboz, Julien (2009), Police Logics and Intelligence Lead Logics in a Risk Society. Information sharing and borders: the role and limits of Frontex, Challenge Deliverable No. 264.

Jeandesboz, Julien and Ragazzi, Francesco (2010), Review of security measures in the Research Framework Programme, PE 432.740, Brussels

Kowslowski, Rey (2005), "Smart Borders, Virtual Borders or No Borders: Homeland Security Choices for the United States and Canada", Law & Bus. Rev. Am., 11(527).

Mitsilegas, Valsamis (2005), "Contrôle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme", Cultures & Conflits, n°58, pp. 155-181.

—————— (2006), Police co-operation: what are the main obstacles to police co-operation in the EU?, PE 378.273, Brussels, 1.1.2006

Parkin, Joanna (2011), The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law, CEPS Liberty and Security paper, April 2011.

Peers, Steve (2008), Proposed new EU Border Control Systems, PE 408.296, Brussels, June 2008.

Salter, Mark, ed. (2010), Mapping Transatlantic Security Relations: The EU, Canada and the War on Terror, London: Routledge.

Scherrer, Amandine, Mégie, Antoine, Mitsilegas, Valsamis (2009), The EU Role in Fighting Transnational Organised Crime, PE 410.678, Brussels, 16.2.2009.

Scherrer, Amandine, Guittet, Emmanuel-Pierre, Bigo, Didier, eds. (2009), Mobilités sous surveillance: Perspectives croisées UE-Canada, Montreal: Athena.

Scherrer, Jeandesboz et al (2011), Developing an EU Internal Security Strategy, fighting terrorism and organised crime, Study for the European Parliament, PE 462.423, C&C, CEPS, Brussels, November 2011.

Schiek, D., Waddington, L. and Bell, M. (eds) (2007), Cases, Materials and Text on National, Supranational and international Non-Discrimination Law, Portland, Oregon: Hart Publishing.

Wiesbrock, A. (2010), Legal Migration to the European Union: Ten Years After Tampere, Martinus Nijhoff Publishers.

Wills, Aidan, Vermeulen, Mathias et al. (2011), Parliamentary oversight of security and intelligence agencies in the European Union, PE 453.207, Brussels, June 2011.

Official documents

Council of Europe (1981), Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981.

—————— (2010), Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, CM/Rec(2010)13, 23 November 2010.

Council of the EU (1997), Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (OJ L 82, 22.3.1997, p. 1)

—————— (2000), Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin OJ L180, 19/07/2000 P. 0022 – 0026.

—————— (2000), Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

—————— (2000), Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316/1, 15.12.2000 (hereafter "Eurodac Regulation").

—————— (2002), Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime as amended by Council Decision 2003/659/JHA and by Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust, Council Document 5347/3/09, Brussels, 15 July 2009.

—————— (2004), Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

—————— (2004), Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Coordination at the External Borders of the Member States of the European Union, OJ L 349/1, 25.11.2004.

—————— (2004), The Hague Programme: strengthening freedom, security and justice in the European Union, 16054/04, Brussels, 13.12.2004.

——————— (2006), Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union, OJ L386/89, 29.12.2006.

——————— (2008), Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6 August 2008, p. 1–11

——————— (2008), Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6 August 2008, p. 12–72.

——————— (2008), Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences OJ L 218/129, 13 August 2008.

——————— (2009), Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ L 121/37, 15.5.2009.

——————— (2009), Draft Council Conclusions on an Information Management Strategy for EU internal security, 16637/09, Brussels, 25.11.2009

——————— (2009), Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, OJ L 325/14, 11.12.2009.

——————— (2010), Draft Internal Security Strategy for the European Union: "Towards a European Security Model", 5842/2/10, Brussels, 23.2.2010

——————— (2010), Council Conclusions on 29 measures for reinforcing the protection of the external borders and combating illegal immigration, 6975/10, Brussels, 1.3.2010.

——————— (2010), Project Group on measure 6, 14011/10, Brussels, 24.9.2010.

——————— (2010), Result of the "Harmony" project - "A generic European Crime Intelligence Model - Bringing together the existing instruments and strengthening Europol's central role, 14851/10, Brussels, 25.10.2010.

——————— (2011), Final report and recommendations of Project Group "Measure 6", doc. 7942/2/11, Brussels, 6 July 2011.

——————— (2012), Note from the French Delegation - Schengen Information System database statistics 01/01/2012, 8281/12, Brussels, 28.3.2012.

——————— (2012), Statistics and reports on automated data exchange for 2011, 11367/12, Brussels, 20.6.2012.

——————— (2012), Europol Work Programme 2012, 13516/11, Brussels, 25.8.2011; Council of the European Union, Europol Work Programme 2013, 12667/12, Brussels, 17.7.2012.

——————— (2012), Note on C.SIS installation and exploitation budget for 2012 and multiannual table of authorised C.SIS installation expenditure, Council Document 14355/12, Brussels, 2 October 2012.

——————— (2012), Draft Regulation of the European Parliament of the Council establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management - Revised compromise proposal by the Presidency, 14357/12, Brussels, 2.10.2012

EDPS (2006), Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final), OJ C 91, 19.4.2006.

—————— (2008), Preliminary Comments on the proposed border package, 3 March 2008.

—————— (2010), Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (2010/C 92/01), OJ C 92/1, 10.4.2010.

—————— (2012), Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] [.....] (Recast version), Brussels, 5.9.2012.

Eurojust (2004), Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, 21 October 2004, OJ C 68/1, 19 March 2005.

European Commission (2005), Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490, 12 October 2005.

—————— (2005), Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, Brussels, 24.11.2005.

—————— (2008), Examining the creation of a European Border Surveillance System (EUROSUR), COM(2011) 68 final, 13.2.2008.

—————— (2008), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing the next steps in border management in the European Union, COM(2008) 69 final, Brussels, 13 February 2008.

—————— (2009), Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], COM(2009) 342 final, Brussels, 10.9.2009.

—————— (2010), Communication to the European Parliament and the Council - Overview of information management in the area of freedom, security and justice, COM(2010)385 final, Brussels, 20 July 2010, p. 31.

—————— (2010), Annual report to the European Parliament and the Council on the activities of the Eurodac Central Unit in 2009, COM(2010) 415 final, 2 August 2010.

—————— (2010), Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final, Brussels, 21 September 2010.

—————— (2010), Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version), COM(2010) 555 final, Brussels, 11.10.2010.

—————— (2010), Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain, COM(2010) 584 final, 20.10.2010.

—————— (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 2.2.2011

—————— (2011), Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program - 17-18 February 2011, SEC(2011) 438 final, Brussels, 16 March 2011.

—————— (2011), Operation of the Council Framework Decision 2006/960/JHA of 18 December 2006 ("Swedish Initiative"), SEC(2011) 593 final, Brussels, 13.5.2011.

—————— (2011), A European terrorist finance tracking system: available options, COM(2011) 429 final, Brussels, 13.7.2011.

—————— (2011), Legislative proposal establishing a legal and technical framework for a European Terrorist Finance Tracking System (EU TFTS), Bussels, July 2011.

—————— (2011), Communication from the Commission to the European Parliament and the Council - Smart borders - options and the way ahead, COM(2011) 680 final, Brussels, 25 October 2011.

—————— (2011), Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011) 1536 final, 12.11.2011

—————— (2011), Impact Assessment accompanying the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SEC(2011) 132 final, Brussels, 2 February 2011.

—————— (2011), Communication "Building an Open and Secure Europe: the home affairs budget for 2014-2020", COM(2011) 749, 15 November 2011.

—————— (2011), Proposal for a Regulation establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa COM(2011) 750, Brussels, 15 November 2011.

—————— (2011), Proposal for a Regulation establishing the Asylum and Migration Fund, COM(2011) 751, Brussels, 15 November 2011.

—————— (2011), Proposal for a Regulation laying down general provisions on the Asylum and Migration Fund and on the instrument for financial support for police cooperation, preventing and combating crime, and crisis management, COM(2011) 752, Brussels, 15 November 2011.

—————— (2011), Proposal for a Regulation establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management, COM(2011) 753, Brussels, 15 November 2011.

—————— (2011), Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR), COM(2011) 873 final, 12.12.2011.

—————— (2011), Roadmap on the legislative proposal establishing a legal and technical framework for a European Terrorist Financing System (EU TFTS), available at: http://ec.europa.eu/governance/impact/planned_ia/docs/2011_home_003_terrorist_finance_tracking_system_tfts_2012_en.pdf (last accessed 14/11/2012)

—————— (2012), Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), COM(2012) 254 final, Brussels, 30.5.2012

—————— (2012), Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit in 2011, COM(2012) 533 final, 21.9.2012.

—————— (2012), Report from the Commission to the European Parliament and the Council - Progress Report on the Development of the Second Generation Schengen Information System (SIS II) – January 2012 to June 2012, COM/2012/587 final, Brussels, 11 October 2010, p. 9.

European Commission against Racism and Intolerance (ECRI) (2007), ECRI General Policy Recommendation No. 11, on combating Racism and Racial Discrimination in Policing, CRI(2007)39, 29 June 2007.

European Data Protection Supervisor (2008), Preliminary Comments on the proposed border package, 3 March 2008

European Parliament (2008), Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)), Rapporteur Sarah Ludford.

—————— (2012), Draft report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 – C7-0039/2011 – 2011/0023(COD)) - Committee on Civil Liberties, Justice and Home Affairs, 2011/0023(COD), Brussels, 14.2.2012.

—————— (2012), Written Question by Sophia In 't Veld No E-007382/2012 of 23 July 2012.

European Parliament and Council of the EU (1995), Directive 95/46/EC of the European Parliament and of the Council 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.

—————— (2006), Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast).

—————— (2006), Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code).

—————— (2006), Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4, 28.12.2006.

—————— (2008), Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218/60, 13.8.2008.

—————— (2011), Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted (recast).

—————— (2011), Regulation No 1168/2011 of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex Regulation).

European Policy Evaluation Consortium (2004), Study for the extended impact assessment of Visa Information System, December 2004.

European Union Agency for Fundamental Rights (2010), Towards More Effective Policing – Understanding and Preventing Discriminatory Ethnic Profiling: A Guide, Vienna.

Europol (2011), Data Protection at Europol, Data Protection Office's brochure, The Hague, 2011, p. 28

—————— (2012), Europol Review 2011, The Hague, September 2012.

Eurostat (2012), International extra-EU air passenger transport by reporting country and partner world regions and countries.

French National Assembly (2004), Report (No 2017) from the Foreign Affairs Committee on the legislative proposal No. 1860, Paris, 22 December 2004 (Rapporteur: Philippe Cochet).

Frontex (2010), Beyond the Frontiers, Warsaw, 2010.

—————— (2011), Frontex General Report 2010, Warsaw.

Future Group (2008), Freedom, Security, Privacy - European Home Affairs in an open world. Brussels, Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, June 2008.

Governmental Accounting Office (2007), Homeland Security: US-VISIT has not fully met expectations and longstanding programme management challenges need to be addressed, GAO-07-4997T, Washington D.C.

———— (2007), Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain, GAO-07-346, Washington D.C.

———— (2009), Homeland Security: Key US-VISIT Components at Various Stages of Completion, but Integrated and Reliable Schedule Needed, GAO-10-13, Washington D.C.

———— (2010), Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options, GAO-10-860, Washington D.C.

———— (2011), Visa Security: Additional Actions Needed to Strengthen Overstay Enforcement and Address Risks in the Visa Process – Statement of Richard M. Stana, Director Homeland Security and Justice Issues, GAO-11-910T, Washington D.C.

Price Waterhouse Coopers (2011), Policy study on an EU Electronic System for Travel Authorisation (EU ESTA) - Final Report, February 2011.

STERIA (2012), Press Release "European Commission deploys Visa Information System developed by Steria-led consortium", 10 September 2012, available on: www.steria.com/sg/media/press-releases/press-releases/article/european-commission-deploys-visa-information-system-developed-by-steria-led-consortium/

United Kingdom Secretary of State for the Home Department (2011), Report to Parliament on the Application of Protocols 19 and 21 to the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) in Relation to EU Justice and Home Affairs Matters (1 December 2009 - 30 November 2010), Cm 8000, January 2011.

Agreements, conventions and declarations

Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82/15, 21 March 2006.

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195/5, 27 July 2010.

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, Official Journal L 186 , 14 July 2012 p. 4-16.

Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, OJ L 215/5, 11 August 2012.

Convention of 19 June 1990 applying the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at their Common Borders. OJ 2000 L 239

Opinion of Advocate General Poiares Maduro on Case C-524/06 "Heinz Huber v Bundesrepublik Deutschland", 3 April 2008

Case law

Court of Justice of the European Union (1986), Case 222/84 Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary, 15 May 1986, ECR 1651.

—————— (2008), Case C-524/06 Heinz Huber v Bundesrepublik Deutschland, 16 December 2008

European Court of Human Rights (1976), Case Handyside v The United Kingdom, 7 December 1976, 1 EHRR 737

—————— (1990), Kruslin v. France, judgment of 24 April 1990, Series A no.176-A, and Huvig v. France, judgment of 24 April 1990, Series A no.176-B

—————— (2000), Rotaru v. Romania, judgment of 4 May 2000, application no. 28341/95

—————— (2008), S and Marper v United Kingdom, 4 December 2008, ECHR 1581

—————— (2009), Rosalind Williams Lecraft v Spain, Comm No. 1493/2006, 30 July 2009

Annex – Analytical table of JHA databases

The analytical table in this Annex lists and compares current and proposed EU JHA databases with regard to: the amount and type of data they process or are expected to process, the possibilities for access they offer and the existing or envisaged interconnections between them. The table is intended to provide the LIBE Committee with a quick reference guide on EU JHA databases, and will also include an overview of incurred and foreseen costs. Of particular salience for the main legal challenges surrounding these systems are questions related to their purpose, personal scope and access to the data.

This Annex aims at providing a comprehensive overview of EU JHA databases. It is not meant to provide a full coverage or account of every existing or planned database or system in the AFSJ. Not every system of information exchange in the Union falls within the scope of this study. Also, publicly available information is often lacking as regards certain components of some of these databases.[1]

The material in this analytical table is organised into four sections:

1) Operational centralised data systems
2) Data systems managed by Member States
3) Data processing schemes established in the context of relations with third countries
4) Data processing operations currently being implemented and/or considered

The main sources used as the background for the analysis include relevant legal instruments setting up or covering the systems and a selected list of previous studies and reports.[2]

[1] Some of the databases not listed here include, as a way of illustration, OLAF Case Management System, ECRIS, EU IntCen and ESTA.

[2] - Scherrer, Jeandesboz et al (2011), Developing an EU Internal Security Strategy, fighting terrorism and organised crime, Study for the European Parliament, PE 462.423, C&C, CEPS, Brussels, November 2011;

- Bigo, Carrera et al (2011), Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament, Study for the European Parliament, PE 453.216, CEPS, Brussels, September 2011;

- European Commission (2010), Communication to the European Parliament and the Council - Overview of information management in the area of freedom, security and justice, COM(2010) 385 final, Brussels, 20 July 2010;

- Hempel, Carius et al (2009), Exchange of information and data between law enforcement authorities within the European Union, Study for the European Parliament, PE 419.590, CEPS, Brussels, April 2009;

- Geyer, Florian (2008), Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice, CEPS Liberty and Security Research Paper No 9, May 2008;

- Hobbing, Peter (2006), An Analysis of the Commission Communication (COM(2005) 597 final) of 24.11.2005 on Improved Effectiveness, Enhanced Interoperability and Synergies among European Databases in the Area of Justice and Home Affairs – Briefing Paper for the European Parliament, PE 378.270, Brussels, February 2006.

1. Operational centralised data systems:

SIS - Schengen Information System[3]	
Type of system	**Centralised** system (C-SIS) with national systems (N-SIS) supplying information.
Purpose	National security, border control and law enforcement purposes
Personal Scope	**EU and non-EU citizens**: • persons wanted for arrest for extradition purposes, • aliens who are reported for the purposes of being refused entry, who have been convicted of an offence carrying a custodial sentence of at least one year and who have committed serious offences or against whom there is genuine evidence of an intention to commit such offences • missing persons or persons in need of police protection • witnesses and persons required to appear before judicial authorities • persons to be put under discreet surveillance or subjected to specific checks.
Scope of information	(a) name and forename, any aliases possibly registered separately; (b) any particular objective and permanent physical features; (c) first letter of second forename; (d) date and place of birth; (e) sex; (f) nationality; (g) whether the persons concerned are armed; (h) whether the persons concerned are violent; (i) reason for the report; (j) action to be taken. **Objects**: vehicles, boats, aircrafts, containers for the purpose of discreet surveillance or specific checks, as well as objects sought for the purposes of seizure or use as evidence in criminal proceedings (stolen identity cards, vehicles, firearms, bank notes).
Size	More than **42 million** entries in January 2012. 40.8 million entries concern objects, 1.2 million concern persons. Among these 1.2 million persons, 692000 concern unwanted aliens.[4]
Retention Period	a) Obligatory necessity review after **1 year** (for discreet surveillance) and after **3 years** (for person tracing). b) **5 years** maximum storage time for vehicles, boats, aircrafts, and containers entered for the purposes of discreet surveillance and specific checks. c) **10 years** maximum storage time for other data than that mentioned under a).
Input	National systems (N-SIS) can input data into the system.
Access	Border authorities, police and customs authorities as well as judicial authorities. Partial access: visa and immigration authorities, Europol and Eurojust.
Data Protection	National data protection rules are applicable. There are national supervisory bodies in each contracting state responsible for the national sections of SIS; and a Joint supervisory authority composed of national supervisory authorities responsible for C-SIS.

[3] See Title IV of the Convention of 19 June 1990 applying the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at their Common Borders. OJ 2000 L 239.

[4] Source: Council of the EU (2012), Note from the French Delegation – Document 8281/12, 28 March 2012.

Costs	**Total budget for C-SIS.I** (from 1991 to 2010): ca. **38 million Euros** C-SIS **Installation Budget** Estimate (2012): ca. **1 million Euros** C-SIS **Operating Budget** Estimate (2012) : ca. **3.8 million Euros**[5]
Participating States	EU-22 (Schengen State Parties) + Non-EU Member States: Norway, Iceland, Switzerland and Liechtenstein. United Kingdom and Ireland are not connected to the current system but have a special status.
Involvement of EU bodies	Operational management of the SIS is carried out in Strasbourg (France) with a backup site in Sankt Johann im Pongau (Austria). Europol and Eurojust may have partial access to the database.

Eurodac[6]	
Type of system	**Centralised** System (within the European Commission) and National Access Points
Purpose	Help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union.
Personal Scope	a) Applicants for asylum (at least 14 years of age) b) Persons apprehended in connection with the irregular crossing of borders coming from a third country c) Aliens found illegally present in a Member State (only for comparison purposes)
Scope of information	• Member State of origin, place and date of the apprehension; • fingerprint data (full 10 fingerprints and 4 control images); • sex; • reference number used by the Member State of origin; • date on which the fingerprints were taken; • date on which the data were transmitted to the Central Unit.
Size	**1 544 558 entries** in December 2009, among them 1 454 315 entries related to asylum applicants, 90 243 entries of persons apprehended at the border and 42 053 persons found illegally present.[7]
Retention Period	a) **10 years** for asylum applicants (data erased if asylum applicant loses that status); b) **2 years** for persons apprehended at borders (data erased if person acquires citizenship, obtains residence permit or leaves EU territory).
Input	National authorities dealing with asylum requests.

[5] Council of the EU (2012), Note on C.SIS installation and exploitation budget for 2012 and multiannual table of authorised C.SIS installation expenditure, Council Document 14355/12, Brussels, 2 October 2012.

[6] Source: Council of the EU, Regulation No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.

[7] European Commission, Annual report to the European Parliament and the Council on the activities of the Eurodac Central Unit in 2009, COM/2010/0415 final, 2 August 2010.

Access	National authorities dealing with asylum requests – In some member states, however, Eurodac is operated partly or entirely by national police services.
Data Protection	Special rules provided in the regulation. Data protection directive 95/46/EC is additionally applicable. EDPS is competent data protection authority to monitor activities of the Eurodac central unit National data protection authorities supervise collection and use of data at member states level.
Costs	The expenditure for maintaining and operating the Central Unit in 2009 was **1.221.183** Euros.[8] Period 2003-2006: **7.8 million Euro** of EU expenditure (externalised activities)
Participating States	EU-27 plus Norway, Iceland, Switzerland and Liechtenstein
Involvement of EU bodies	Database manager is the **European Commission**. As of December 2012, the database manager for Eurodac is the **European agency for the operational management of large-scale IT systems** in the area of freedom, security and justice, located in Tallinn, Estonia. **EDPS** has special role in checking data protection rules of central database.

CIS - Customs Information System[9]

Type of system	**Centralised** CIS, located in Brussels
Purpose	To assist in combating customs related crime by facilitating co-operation between European customs authorities
Personal Scope	**1) "Traditional" CIS:** Information on persons (for specific purposes of sighting and reporting, discreet surveillance or specific checks and only if, especially on the basis of prior illegal activities, there is evidence to suggest that the person concerned has committed, is committing or will commit actions which are in breach of customs or agricultural legislation.) **2.) Customs Files Identification Database (FIDE):** Information on ongoing or completed investigations for serious infringements of national laws against persons or businesses in member states.
Scope of information	• business name; • trading name; • address of the business; • VAT identification number of the business; • excise duties identification number; • information as to whether the VAT identification number and/or the excise duties identification number is in use; • names of the managers, directors and, if available, principal shareholders of the business;

[8] *Ibidem*.

[9] Source: Council of the EU, Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (OJ L 82, 22.3.1997, p. 1).

	• number and date of issue of the invoice; and • amount invoiced.
Size	As of 31 May 2007 there were: - **1431** third pillar active ("existing") users - **376** third pillar active cases, - **7094** third pillar queries[10]
Retention Period	**For traditional CIS:** As long as necessary to achieve the purpose for which the data was included. After **1 year** an obligatory review of the necessity to keep the data must take place. **For FIDE:** Maximum **3 years** if no infringement has been established – Maximum **6 years** if infringement but no conviction or fine – Maximum **10 years** if conviction or fine ensued.
Input	Inclusion of data is governed by national laws of member states.
Access	Customs administrations as designated by member states. Data retrieved from the system may also be used by other national authorities than those who have direct access, by non-member states and by international or regional organisations.
Data Protection	National data protection rules are applicable. There are national supervisory bodies in each Member State responsible for the lawfulness of the entry, processing and use of CIS data in that member state; and a Joint supervisory authority composed of national supervisory authorities responsible for CIS operations.
Costs	**4.75 million** Euros in total for the Anti-Fraud Information System, which includes the FIDE (2005).[11]
Participating States	EU-27
Involvement of EU bodies	Database manager is the **European Commission**.

EUROPOL Information System[12]

Type of system	**Centralised** system: a platform to store personal information on persons suspected or convicted of crimes for which Europol is competent.
Purpose	Fight against cross-border crime
Personal Scope	**EU and non-EU citizens:** a) Suspects or convicted persons of a crime. b) Possible future offenders.

[10] Report of the Joint Supervisory Authority of Customs presenting a general overview of the use of the Customs Information System by the Member States, Brussels, 18 December 2007.

[11] French National Assembly, Report (No 2017) from the Foreign Affairs Committee on the legislative proposal No. 1860, Paris, 22 December 2004 (Rapporteur: Philippe Cochet).

[12] Council of the EU (2009), Decision of 6 April 2009 establishing the European Police Office (Europol), OJ L 121, 15.5.2009, p. 37–66.

Scope of information	• surname, maiden name, given names and any alias or assumed name; • date and place of birth; • nationality; • sex; • place of residence, profession and whereabouts of the person concerned; • social security numbers, driving licences, identification documents and passport data; and • where necessary, other characteristics likely to assist in identification, including any specific objective physical characteristics not subject to change such as dactyloscopic data and DNA profile (established from the non-coding part of DNA). • criminal offences, alleged criminal offences and when, where and how they were (allegedly) committed; • means which were or may be used to commit those criminal offences including information concerning legal persons; • departments handling the case and their filing references; • suspected membership of a criminal organisation; • convictions, where they relate to criminal offences in respect of which Europol is competent; • inputting party.
Size	**183 240** objects and **41 193** persons (December 2011).[13]
Retention Period	As long as necessary for the performance of Europol's task. After a maximum of **3 years** an obligatory review of the necessity to keep the data must take place. Personal data relating to specific offences shall be deleted if proceedings against the person are dropped or if that person is acquitted of the offence.
Input	Member states, represented by their national units and liaison officers in compliance with their national procedures, may feed data into the system. Europol itself shall input data supplied by third states and third bodies as well as analysis data.
Access	National units, liaison officers, the Director, the Deputy Directors as well as duly empowered Europol officials may have access to the system. Indirect access by "competent authorities" designated by member states is also possible.
Data Protection	National supervisory body in each member state responsible for monitoring the input and use of Europol data by the member state's authorities. Joint supervisory authority composed of national supervisory authorities responsible for Europol. Also, the Data Protection Office in Europol has a specific role of conducting regular audits on Europol's databases.[14]
Costs	In 2011 the Europol budget was **84.8 million** Euros.[15]
Participating States	EU-27. Europol also hosts staff from partner organisations from third-countries, among them the USA (US Secret Service, DEA, and FBI) as well as Colombia and Canada.
Involvement of EU bodies	Europol may associate experts from the agencies listed in Article 22 of the Europol Decision: **Eurojust**, **OLAF**, **Frontex**, **CEPOL**, **ECB** and **EMCDDA** although it is not clear if these experts have access to the Europol Information System.

[13] See Europol (2012), Europol Review 2011, The Hague, September 2012.

[14] See Europol (2011), Data Protection at Europol, Data Protection Office's brochure, The Hague, 2011, p. 28.

[15] Europol Review 2011 (*op. cit.*).

EUROPOL Analytical Work Files (AWF)[16]	
Type of system	**Centralised** system: stores a wider set of data perceived as necessary to provide operational analysis to aid investigations and operations carried out by the Member States.
Purpose	Fight against cross-border crime - Analysis work files shall be opened for the purposes of analysis defined as the assembly, processing or use of data with the aim of assisting criminal investigations.
Personal Scope	**EU and non-EU citizens:** a) Suspects or convicted persons of a crime. b) Possible future offenders. c) Possible witnesses. d) Victims and possible victims. e) Contacts and associates. f) Persons who can provide information on the criminal offence under consideration.
Scope of information	**For suspects, convicted persons, possible future offenders and contacts and associates:** Personal details, physical description, ID numbers, biometrics, information on occupation and skills, behavioural data, means of communication and of transport, previous criminal activities, links with other databases, etc.[17] **For victims and possible victims:** Personal details, physical description, ID numbers, biometrics, victim identification data, reason for victimisation, information on the crime and on the court case, etc. **For possible witnesses:** Personal details, physical description, ID numbers, biometrics, information on the crime and on the court case, information on the anonymity and the protection offered to the witness (and by whom), new identity, etc. **For persons who can provide information on the criminal offence under consideration:** Personal details, physical description, ID numbers, biometrics, coded personal details, information on the crime and on the court case, type of information that the person supplied, information on the anonymity and the protection offered to the witness (and by whom), new identity, negative experiences, financial rewards of favours, etc.
Size	Previously, the AWF concept was based on **23 different AWFs** which meant 23 disconnected databases. The new AWF concept foresees two AWFs: **AWF SOC** on Serious Organised Crime and **AWF CT** on Counter-Terrorism.[18]
Retention Period	As long as necessary for the performance of Europol's task. After a maximum of **1 year** an obligatory review of the necessity to keep the data must take place.

[16] See Council of the EU (2009) (*op. cit.*) as well as Council of the EU (2009), Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, OJ L 325/14, 11 December 2009.

[17] The full list of personal data categories that may be processed can be found in article 6(2) of Council Decision 2009/936/JHA (*op. cit.*).

[18] Drewer, Ellerman (2012), Europol's data protection framework as an asset in the fight against cybercrime, ERA Forum, Volume 13, Issue 3, November 2012, pp 381-395.

Input	Analysts and other Europol official specifically designated for each analysis project. Experts from third states and third bodies may be "associated" with the activities of an analysis group.
Access	Analysts and other Europol officials specifically designated for each analysis project. The liaison officers and/or experts of the member states which are concerned by the analysis file. Experts from third states and third bodies may be "associated" with the activities of an analysis group.
Data Protection and Control	National supervisory body in each member state responsible for monitoring the input and use of Europol data by the member state's authorities. Joint supervisory authority composed of national supervisory authorities responsible for Europol. Also, the Data Protection Office in Europol has a specific role of conducting regular audits on Europol's databases.[19]
Costs	In 2011 the Europol budget was **84.8 million** Euros.[20]
Participating States	EU-27. Any Third State which has concluded an operational agreement with Europol may participate in an AWF to the full extent that a Member State can. Third States without an operational agreement may contribute data to an AWF but may not participate beyond that. The same applies to International Organisations and other third parties.
Involvement of EU bodies	Europol may associate experts from the agencies listed in Article 22 of the Europol Decision: **Eurojust**, **OLAF**, **Frontex**, **CEPOL**, **ECB** and **EMCDDA**.

EUROJUST[21]

Type of system	**Centralised** Case Management System (CMS): secure storage of casework data and exchange with national members. The CMS is composed of temporary work files and of an index which contain personal and non-personal data.
Purpose	• support the management and coordination of investigations and prosecutions for which Eurojust is providing assistance, in particular by the cross-referencing of information; • facilitate access to information on ongoing investigations and prosecutions; • facilitate the monitoring of lawfulness and compliance with the provisions of this Decision concerning the processing of personal data.
Personal Scope	**EU and non-EU citizens:** a) Persons who are the subject of criminal investigation or prosecution. b) Witnesses or victims in a criminal investigation or prosecution. c) Other personal data relating to the circumstances of an offence where they are immediately relevant to and included in ongoing investigations (in exceptional cases).

[19] See Europol (2011), Data Protection brochure (*op. cit.*)

[20] Europol Review 2011 (*op. cit.*).

[21] Council of the EU (2002), Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime as amended by Council Decision 2003/659/JHA and by Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust, Council Document 5347/3/09, Brussels, 15 July 2009.

Scope of information	**For suspects and convicted persons:** • Personal details: surname, first name, given names, date and place of birth, nationality, sex; • place of residence, profession and whereabouts of the person concerned; • social security numbers, driving licences, identification documents and passport data; • information concerning legal persons; • bank accounts and accounts with other financial institutions; • description and nature of the alleged offences, the date on which they were committed, the criminal category of the offences and the progress of the investigations; • the facts pointing to an international extension of the case; • details relating to alleged membership of a criminal organisation; • telephone numbers and e-mail addresses; • vehicle registration data; • DNA profiles established from the non-coding part of DNA, photographs and fingerprints. **For witnesses and victims:** • Personal details: surname, first name, given names, date and place of birth, nationality, sex; • place of residence, profession and whereabouts of the person concerned; • description and nature of the offences involving them, the date on which they were committed, the criminal category of the offences and the progress of the investigations.
Size	In 2011, Eurojust registered **1441 cases**.
Retention Period	In general, personal data shall be stored as long as prosecution is ongoing, has not resulted in a final judicial decision and is still legally possible (e.g. not statute barred). When one of the deadlines above has expired, Eurojust shall review the need to store the data longer in order to achieve its objectives. Continuous observance is required, with an obligatory review of necessity every **3 years**.
Input	Eurojust national members, their assistants and authorised Eurojust staff.
Access	Eurojust national members, their assistants and authorised Eurojust staff (including the Data Protection Officer). Eurojust may exchange data with national competent authorities of member states, authorities of third countries which are competent for investigations and prosecutions as well as international organisations and bodies.
Data Protection	Own data protection officer as well as independent supervisory authority. Own extensive rules of procedure on the processing and protection of personal data at Eurojust were adopted in 2004.[22]
Costs	Total budget of Eurojust in the year 2011: **31.7 million Euros**.
Participating States	EU-27. Eurojust has also concluded agreements with a number of third countries, such as Croatia, Iceland, Switzerland, Norway, USA and FYROM).
Involvement of EU bodies	The **European Judicial Network** and Eurojust have strong links – the EJN Secretariat forms part of Eurojust's staff and Eurojust may inform EJN contact points about ongoing cases. Agreements and working arrangements have been concluded between Eurojust and the **European Commission** (DG Justice), **Europol**, **OLAF**, **CEPOL**.

[22] College of Eurojust (2004), Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, 21 October 2004, OJ C 68/1, 19 March 2005.

VIS – Visa Information System[23]	
Type of system	**Centralised** system with communication infrastructure to national systems and consulates in third countries. The VIS is composed of two systems: the VIS central database and an Automated Fingerprint Identification System (AFIS).
Purpose	• to facilitate the visa application procedure; • to prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application; • to facilitate the fight against fraud; • to facilitate checks at external border crossing points and within the territory of the Member States; • to assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States; • to facilitate the examinations of asylum applications; • to contribute to the prevention of threats to the internal security of any of the Member States.
Personal Scope	**Visa applicants (TCNs)**, as well as (indirectly) **EU citizens** who are hosts/sponsors of a visa applicant. Exceptions: • Children under the age of twelve; • Persons for whom fingerprinting is physically impossible; • Heads of state or government and members of a national government with accompanying spouses, and the members of their official delegation, when officially visiting; • Sovereigns and other senior members of a royal family, when officially visiting.
Scope of information	Data relating to short-stay visa applications (up to three months): • alphanumeric data contained in the Schengen visa application form (name, nationality, place of residence, occupation, travel document number, type of visa requested, main destination and duration of stay, border of first entry, details of the inviting person), • a digital photograph, • ten fingerprints taken of the applicant, • links to previous visa applications and to the application files of persons travelling together, • and information on the official decision on the visa application (issuance, refusal, annulment, revocation, extension).
Size	Since the start of operations in October 2011, the VIS has processed approx. **1 million visa applications**.[24] Foreseen capacity: **70 million applicants** (2004).
Retention Period	**5 years** maximum. Automatic deletion of the data if applicant acquires nationality of a participating state.

[23] The VIS started operations in October 2011 in Schengen States' consulates in North Africa and was progressively deployed in the Near East and the Gulf Region in 2012. Legal framework: European Parliament and Council of the EU (2008), Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) as amended by Regulation (EC) No 810/2009 of 13 July 2009.

[24] Source: STERIA (2012), Press Release "European Commission deploys Visa Information System developed by Steria-led consortium", 10 September 2012, available on: www.steria.com/sg/media/press-releases/press-releases/article/european-commission-deploys-visa-information-system-developed-by-steria-led-consortium/

Input	Visa authorities of the participating states.
Access	a) Visa, immigration and asylum authorities. b) Competent authorities responsible for carrying out checks at external border crossing points in accordance with Schengen Border Code. c) Designated authorities dealing with terrorist offences and other serious criminal offences, in specific cases only. d) Europol (within the limits of its mandate and when necessary to perform its tasks). e) Third countries or international organisations (under specific circumstances)
Data Protection	Mix of EU and national data protection rules. National supervisory authorities in each contracting state shall monitor the lawfulness of the processing of VIS data on their territory. EDPS shall monitor the activities of the EU personnel managing VIS.
Costs	The Commission was in charge of the development of the central database, the national interfaces and the communication infrastructure between the central VIS and the national interfaces. Their development was funded by the EU budget (the cost amounted to **€135 million between 2004 and 2011**). Each Schengen state is responsible for the development, management, and operation of its national system.
Participating States	All Schengen States: EU-22 (Denmark has decided to opt in) + Non-EU Member States: Norway, Iceland, Switzerland and Liechtenstein which is due to join very shortly. United Kingdom and Ireland have opted out.
Involvement of EU bodies	As of December 2012, the database manager for VIS is the **European agency for the operational management of large-scale IT systems** in the area of freedom, security and justice, located in Tallinn, Estonia. **EDPS** has special role in checking data protection rules of central database. **Europol** can have access to VIS for the purpose of fighting terrorism and organised crime.

SIS II (not yet operational)[25]

Type of system	SIS II is composed of: • a **central** system ("Central SIS II"); • a **national** system (the "N.SIS II") in each Member State, consisting of the national data systems which communicate with Central SIS II. An N.SIS II may contain a data file (a "national copy"), containing a complete or partial copy of the SIS II database; • a communication infrastructure between the central and the national systems that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux.
Purpose	To ensure a high level of security within the EU's AFSJ, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of the Treaty relating to the movement of persons in their territories, using information communicated via this system.
Personal Scope	**EU and non-EU citizens:** a) Persons wanted for arrest for surrender purposes on the basis of a European arrest warrant or wanted for arrest for extradition purposes. b) Third country nationals to be refused entry into the Schengen territory.

[25] European Parliament and Council of the EU (2006), Regulation (EC) No 1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, p. 4-23.

	c) Missing persons. d) Witnesses and persons required to appear before judicial authorities. e) Persons to be put under discreet checks or subjected to specific checks. f) Vehicles, boats, aircrafts, containers for the purpose of discreet checks or specific checks. g) Objects sought for the purposes of seizure or use as evidence in criminal proceedings (stolen identity cards, vehicles, firearms, bank notes).
Scope of information	• Personal details: surname, first name, given names, date and place of birth, nationality, sex; • any specific, objective, physical characteristics not subject to change; • photographs and fingerprints; • whether the person concerned is armed, violent or has escaped; • authority issuing the alert, reason for the alert, link(s) to other alerts issued in SIS II and action to be taken.
Size	Estimates provided in official documents refer to searches conducted in the system, not to total number of entries. In January 2010 the existing system contained **31 million entries**. It is agreed that the system capacity at go-live should be **70 million alerts** and that SIS II should be tested to a capacity of **100 million alerts**, without the need for technical change.
Retention Period	a) After a maximum of **3 years** an obligatory review of the necessity to keep the data must take place (after **1 year** in case of entry for discreet check or specific checks). However, under certain circumstances, even after deletion of data in the SIS II, contracting states are allowed to store data for a longer period in their national files. b) **10 years maximum** storage time for alerts on objects for seizure or use as evidence in criminal proceedings. c) **5 years maximum** storage time for vehicles, boats, aircrafts, and containers entered for the purposes of discreet checks and specific checks.
Input	Information is supplied by contracting states via national interfaces (NI-SIS).
Access	**Full access**: Authorities responsible for the identification of third country nationals for the purposes of border control, other police and customs checks carried out within the country and judicial authorities as designated by the contracting states. **Partial access**: visa and immigration authorities, vehicle registration authorities, Europol, Eurojust. **Information exchange** may be possible with Interpol.
Data Protection	Mix of EU and national data protection rules. National supervisory authorities in each contracting state shall monitor the lawfulness of the processing of SIS II data on their territory. European Data Protection Supervisor shall monitor the activities of the EU personnel managing SIS II. All supervisory bodies shall meet at least twice a year.
Costs	By the end of **June 2012** the total budgetary commitments made by the Commission on the SIS II project, since 2002, amounted to **just under €150 million.**[26]
Participating States	EU-22 (Schengen State Parties) + United Kingdom and Ireland (partially) + Non-EU Member States: Norway, Iceland, Switzerland and Liechtenstein. The United Kingdom and Ireland participate in the police cooperation aspects of the Schengen Convention and SIS II, with the exception of alerts relating to third country nationals.[27]
Involvement of EU bodies	It is expected that, as of March 2013, the database manager for SIS II will be the **European agency for the operational management of large-scale IT systems** in the area of freedom, security and justice, located in Tallinn, Estonia. **EDPS** has special role in checking data protection rules of central database. **Europol** and **Eurojust** will be able to access some data.

[26] European Commission (2012), Report from the Commission to the European Parliament and the Council - Progress Report on the Development of the Second Generation Schengen Information System (SIS II) – January 2012 to June 2012, COM/2012/587 final, Brussels, 11 October 2010, p. 9.

[27] Parkin, Joanna (2011), The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law, CEPS Liberty and Security paper, April 2011, p. 4.

2. Data-processing schemes managed at Member State level:

API - Advanced Passenger Information[28]	
Type of system	**De-centralised**: carriers transfer the data to national authorities dealing with border controls.
Purpose	Improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities.
Personal Scope	**Air passengers** crossing an external border of the EU, **both EU and non-EU citizens.**
Scope of information	Number and type of travel document used, nationality, full names, date of birth, border crossing point of entry, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport, and initial point of embarkation.
Size	Variable as it is a decentralised database. Could concern up to **300 million passengers annually** (in 2010, 296 320 043 passengers flew in extra-EU flights).[29] The European Commission provided statistics for one Member State (United Kingdom) in 2009: **379 persons** were refused entry and **56 ID documents** that were lost, stolen or cancelled were impounded following the use of the API system.[30]
Retention Period	For national authorities: **24 hours** after transmission, with possibilities to keep it longer. For air carriers: **24 hours** after landing
Input	Air carriers.
Access	Authorities responsible for carrying out checks on persons at external borders. API is in force in each Member State, but only a few of them use it.[31]
Data Protection	Directive 95/46/EC, national rules – passengers must be informed by carriers about their data and carriers must delete the data after 24 hours..
Costs	Estimation of setting up costs for a big Member State (soft and hardware) for API and PNR: **250 million Euros**. 70% of these costs relate to API so the estimated total cost for a big Member State to implement API is **175 million Euros**.[32]
Participating States	EU-27 + Non-EU States: Norway, Iceland, Switzerland and Liechtenstein
Involvement of EU bodies	N/A

[28] Council of the EU (2004), Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

[29] Source: Eurostat (2012), International extra-EU air passenger transport by reporting country and partner world regions and countries.

[30] European Commission (2010), Communication to the European Parliament and the Council - Overview of information management in the area of freedom, security and justice, COM(2010)385 final, Brussels, 20 July 2010, p. 31.

[31] *Ibidem*, p. 45.

[32] Source: European Commission (2011), Commission Staff Working Paper - Impact Assessment accompanying the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SEC(2011) 132 final, Brussels, 2 February 2011, p. 45.

Swedish Initiative[33]	
Type of system	**Decentralised system** - national contact points designated by Member States handle urgent requests for information.
Purpose	Exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.
Personal Scope	Any existing information or criminal intelligence available to law enforcement authorities (may include personal data of any **EU and non-EU citizen**).
Scope of information	Any type of information or data which is held by law enforcement authorities as well as any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities. May include the circumstances in which the offence was committed, the nature of the offence and the identity of the person being the main subject of the criminal investigation.
Size	Number of "Swedish Initiative" requests sent via Europol's Secure Information Exchange Network Application (SIENA) for the years 2009, 2010 and 2011: **111**.[34] (Other channels include SIRENE, Interpol and national bilateral channels).
Retention Period	National rules on time limits apply.
Input	Police, customs and any other authority with the power to investigate crime.
Access	Police, customs and any other authority with the power to investigate crime.
Data Protection	National data protection rules, as well as Council of Europe Convention 108 on data protection, Council of Europe Additional Protocol 181 and Council of Europe Police Recommendation No R (87) 15 are applicable.
Costs	N/A
Participating States	EU-27 plus Norway, Switzerland and Iceland.
Involvement of EU bodies	Information may be exchanged with **Europol** and **Eurojust** if it falls within the scope of their respective mandates.

[33] Council of the EU (2006), Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89.

[34] See European Commission (2011), Staff Working Paper on the Operation of the Council Framework Decision 2006/960/JHA of 18 December 2006 ("Swedish Initiative"), SEC(2011) 593 final, Brussels, 13 May 2011, p. 7.

Prüm scheme[35]	
Type of system	**De-centralised system**, hit/no hit system.
Purpose	Making the essential parts of the Prüm Treaty of 27 May 2005 applicable to all member states. Networking member states national databases. Developing common procedures among member states in the field of police and judicial cooperation in criminal matters.
Personal Scope	**EU and non-EU citizens:** • **DNA analysis files** for investigation of criminal offences (hit/no hit system). • **Dactyloscopic (fingerprint) data** for prevention and investigation of criminal offences (hit/no hit system). • **Owners or operators** linked to vehicle registration data for prevention and investigation of criminal offences.
Scope of information	**DNA**: non-coding part of DNA and anonymous data only, with a reference number. **Fingerprints**: dactyloscopic data (anonymous) and a reference number. **Vehicle Registration Data**: data relating to owners or operators; and data relating to vehicles (including full chassis number and full registration number).
Size	Statistics have been provided by the General Secretariat of the Council[36] but the actual figures are not available to the public at the time of finalising this study.
Retention Period	Allowed storage time is linked to specific purposes; maximum period for keeping data is **determined by national law** of the supplying member state.
Input	National contact points designated by Member States.
Access	Domestic access is governed by national law.
Data Protection	National data protection provisions apply (individuals may turn to their national data protection supervisor to enforce their rights concerning the processing of personal data).
Costs	N/A
Participating States	EU-27, Norway and Iceland are about to accede to this instrument (2010).[37]
Involvement of EU bodies	EUROPOL provides a helpdesk service for the exchange of information between Member States (Prüm Helpdesk). EUROPOL Secure Information Exchange Network Application (SIENA) can be used to exchange information under the Prüm scheme.

[35] Council of the EU (2008), Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6 August 2008, p. 1–11 as well as Council of the EU (2008), Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6 August 2008, p. 12–72.

[36] Council of the EU (2012), Council Decisions 2008/615/JHA and 2008/616/JHA of 23 June 2008 - statistics and reports on automated data exchange for 2011, Document No. 11367/12, Brussels, 20 June 2012.

[37] European Commission (2010) Communication on Overview of information management (*op. cit.*), p. 47.

3. Data processing schemes established in the context of relations with third countries:

PNR (Passenger Name Record) Agreements with Canada[38], Australia[39] and the United States[40]	
Type of system	**De-centralised system**: Transfer of PNR data to third-countries through agreements concluded with Canada (2006), Australia (2011) and the United States (2012). Other third-countries have started requesting PNR data from airlines, which could lead to similar agreements: Japan, South Korea, Qatar[41] and New Zealand.[42]
Purpose	**EU-Canada**: "preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime" **EU-Australia**: "for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime" **EU-United States**: "for the purpose of preventing, detecting, investigating and prosecuting: • terrorist offences and related crimes • Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature"
Personal Scope	**All passengers (EU and non-EU citizens)** using air transportation between Europe and the United States, Australia, Canada (both ways). The EU-United States agreement shall also apply to carriers incorporated or storing data in the European Union and operating passenger flights to or from the United States.
Scope of information	**EU-Australia and EU-United States agreements:** 1. PNR record locator code 2. Date of reservation/issue of ticket 3. Date(s) of intended travel 4. Name(s) 5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.) 6. Other names on PNR, including number of travellers on PNR 7. All available contact information (including originator information) 8. All available payment/billing information 9. Travel itinerary for specific PNR

[38] European Union (2006), Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82/15, 21 March 2006.

[39] European Union (2011), Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, Official Journal L 186 , 14 July 2012 p. 4-16.

[40] European Union (2012), Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, OJ L 215/5, 11 August 2012.

[41] See European Parliament (2012), Written Question by Sophia In 't Veld No E-007382/2012 of 23 July 2012 and the answer given by Commissioner Malmstrom on 24 September 2012.

[42] European Commission (2010), Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final, Brussels, 21 September 2010, p. 2.

	10. Travel agency/travel agent 11. Code share information 12. Split/divided information 13. Travel status of passenger (including confirmations and check-in status) 14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote 15. All baggage information 16. Seat information, including seat number 17. General remarks including OSI, SSI and SSR information 18. Any collected APIS information 19. All historical changes to the PNR listed under points 1 to 18 **EU-Canada agreement:** 1. All of the above 2. No show history 3. Go show information 4. Standby 5. Order at check in
Size	Similar to the API, the size of the PNR data transferred is variable as it depends on the number of passengers flying between the EU and Canada, Australia and the USA. In 2010, **9.3 million passengers** flew between Canada and the EU; **34 000** between Australia and the EU, and **48.5 million** between the US and the EU.[43]
Retention Period	**EU-Canada** PNR agreement: provides for a regular storage time of **3.5 years** and exceptionally a maximum of **6 years**. **EU-Australia** PNR agreement: provides for a maximum retention time of **5.5 years**. **EU-United States** PNR agreement: the regular storage time is of **10 years** for crime, **15 years** for terrorist offences.
Input	Air carriers.
Access	The **US Department of Homeland Security**, the **Canada Border Services Agency** and the **Australian Customs Services**, which may share data with domestic law enforcement and counter-terrorism services.
Data Protection	Applicable rules on data protection, access and correction requests by data subjects are found in the agreements themselves.
Costs	N/A
Participating States	EU-27 and Canada, Australia and the United States.
Involvement of EU bodies	N/A

[43] Source: Eurostat (2012), *op. cit.*

EU-US TFTP (Terrorist Finance Tracking Programme)[44]	
Type of system	**De-centralised system**: transfer of financial payment messages and financial information from the EU to the United States by providers of international financial payment messaging services (currently the Belgian company SWIFT – Society for Worldwide Interbank Financial Telecommunication).
Purpose	Prevention, investigation, detection, or prosecution of terrorism or terrorist financing.
Personal Scope	**Originator** and **recipient** of a financial transaction (**EU citizens and foreigners**).
Scope of information	The requests by US authorities shall be "tailored as narrowly as possible in order to minimise the amount of data requested". According to a Commission report,[45] the following data was requested in the first 6 months after the entry into force of the Agreement: • Financial messages, • Relevant time-period of the messages, • Geographical scope of the messages, • Name(s), • Account number(s), • Address(es), • National identification number(s). In exceptional circumstances, personal data revealing racial or ethnic origin, political opinions, or religious or other beliefs, trade union membership, or health and sexual life may be extracted.
Size	Information on the number of data requested, transferred and the number of searches made in the context of the EU-US TFTP Agreement is not made public as it would allow terrorists to "undermine the effectiveness of the program".[46] The US Department of Treasury provides a general number of all financial payment messages accessed by TFTP analysts from August 2010 to January 2011: **27 006**.[47]
Retention Period	**5 years** after reception, annual evaluation of the necessity to keep data for combating terrorism or its financing.
Input	**SWIFT**, or any other provider of international financial payment messaging services as identified in the annex of the Agreement (can be updated via diplomatic notes).
Access	**United States Treasury Department**. Information extracted from the data may be exchanged with **law enforcement, public security, or counter terrorism authorities** in the United States, Member States, or third countries, or with **Europol** or **Eurojust**, or other appropriate international bodies

[44] European Union (2010), Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195/5, 27 July 2010.

[45] European Commission (2011), Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program - 17-18 February 2011, SEC(2011) 438 final, Brussels, 16 March 2011.

[46] *Ibidem*, p. 6-7.

[47] *Ibidem*, p. 18.

Data Protection	• The data is held in a secure physical environment, there can be no unauthorised access to the data, the data are not interconnected with any other database, the provided data shall not be subject to any manipulation, alteration or addition, and no copies of provided data should be made, other than for recovery back-up purposes. • Search of the data needs to be "narrowly tailored". Independent overseers, appointed by SWIFT, as well as one independent overseer appointed by the European Commission, see and verify all the searches performed on the provided data. They have the power to block searches to request more information and have used it more than once in 2011.[48] • Articles 15 and 16 of the Agreement provide for individuals' rights to access, rectification, erasure or blocking of their data.
Costs	N/A
Participating States	EU-27 (United Kingdom, Ireland and Denmark have the possibility to opt-out of the Agreement according to Article 22). United Kingdom has decided to opt in.[49]
Involvement of EU bodies	**Europol** is responsible for checking that the data requested is "tailored as narrowly as possible" by US authorities. An **independent overseer**, appointed by the European Commission, reviews in real time and retrospectively all searches made on the data.

EU PNR system (under negotiation)[50]

Type of system	**Decentralised system** of national Passenger Information Units.
Purpose	Prevention, detection, investigation and prosecution of terrorist offences and serious crime
Personal Scope	**All passengers (EU and non-EU citizens)** using air transportation to cross the external borders of the Member States of the EU.
Scope of information	(1) PNR record locator (2) Date of reservation/issue of ticket (3) Date(s) of intended travel (4) Name(s) (5) Address and contact information (telephone number, e-mail address) (6) All forms of payment information, including billing address (7) Complete travel itinerary for specific PNR (8) Frequent flyer information (9) Travel agency/travel agent (10) Travel status of passenger, including confirmations, check-in status, no show or go show information

[48] *Ibidem*, p.10.

[49] United Kingdom Secretary of State for the Home Department (2011), Report to Parliament on the Application of Protocols 19 and 21 to the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) in Relation to EU Justice and Home Affairs Matters (1 December 2009 - 30 November 2010), Cm 8000, January 2011, p. 4.

[50] European Commission (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2 February 2011.

	(11) Split/divided PNR information (12) General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent) (13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields (14) Seat number and other seat information (15) Code share information (16) All baggage information (17) Number and other names of travellers on PNR (18) Any Advance Passenger Information (API) data collected (19) All historical changes to the PNR listed in numbers 1 to 18
Size	Variable as it is a decentralised database. Could concern up to **300 million passengers** annually (in 2010, 296 320 043 passengers flew in extra-EU flights).[51]
Retention Period	**30 days** retention in the database of the Passenger Information Unit. After expiry of these 30 days, **5 years** retention period in a "masked out" state (anonymous data and limited access). After these 5 years, data should be deleted unless relevant for current investigation: in that case, national retention rules apply.
Input	Air carriers.
Access	Passenger Information Units responsible for collecting PNR data from the air carriers, storing them, analysing them and transmitting the result of the analysis to the competent authorities determined by each Member State. Competent authorities: authorities competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime.
Data Protection	• Prohibition of the processing of PNR data revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life. • Obligation by air carriers to inform passengers about PNR data transfer. • Assurance for every passenger to have the same right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as under national law.
Costs	Estimations range from **0.10 Euro** to **0.17 Euro** per passenger.[52]
Participating States	EU-24: Denmark will not be bound by the new rules, United Kingdom and Ireland will need to give notification as to whether they want to opt-in or not. Possibility to transfer PNR data to third countries.
Involvement of EU bodies	EUROPOL's SIENA can be used for exchanges of information included under Article 7 of the current proposal (Art. 8(6)).

[51] Source: Eurostat (2012), *op. cit.*

[52] Hernanz, Nicholas (2012), More Surveillance, More Security? The Landscape of Surveillance in Europe and Challenges to Data Protection and Privacy – Policy Report on the Proceedings of a Conference at the European Parliament, SAPIENT Deliverable 6.4, January 2012, p. 7.

EU TFTS (Terrorist Finance Tracking System, under consideration)[53]	
Type of system	Data system (similar to TFTP) extracting and storing financial information on EU territory for the purpose of combating terrorism. The European Commission presented available options for an EU TFTS in 2011: a **centralised European approach,** a **de-centralised national approach** and a **hybrid system** were discussed.
Purpose	1) ensuring an effective instrument to prevent and to fight the financing of terrorism, and 2) limiting personal data flow to third countries
Personal Scope	Same as EU-US TFTP: **originator** and **recipient** of a financial transaction. **All EU citizens and foreigners** making use of banking services in the EU can conceivably be affected.[54]
Scope of information	This was not discussed in the Communication.
Size	N/A
Retention Period	This was not discussed in the Communication.
Input	All providers of international financial payment messaging services (not only SWIFT as is the case in the EU-US TFTP Agreement).
Access	If de-centralised system: national law enforcement authorities would be involved for verifying and authorising requests for searches. If centralised EU system: Europol would store the data and have access to it. Eurojust would be involved as well.
Data Protection	If de-centralised system: national data protection rules should apply. If centralised EU system: **Europol** would store the data and deal with requests by data subjects for **access**, **rectification** and **blocking**, all in accordance with its existing legal framework and EU data protection provisions.
Costs	**33-47 million Euro** initial set-up costs, with an additional **7-11 million Euro** required for annual running costs.
Participating States	EU-27, United States and other third countries.
Involvement of EU bodies	Data storage could take place either at the national or EU level. At the EU level, it could take place at **Europol** or at another EU body, such as the **Agency for the operational management of large-scale IT systems**.

[53] European Commission (2011), Communication to the European Parliament and the Council - A European terrorist finance tracking system: available options, COM(2011) 429 final, Brussels, 13 July 2011

[54] European Commission (2011), Roadmap on the legislative proposal establishing a legal and technical framework for a European Terrorist Financing System (EU TFTS), available at (last accessed 14/11/2012): http://ec.europa.eu/governance/impact/planned_ia/docs/2011_home_003_terrorist_finance_tracking_system_tfts_2012_en.pdf

4. Data processing operations currently being implemented and/or considered:

Frontex Information System (currently being implemented)[55]	
Type of system	The Frontex Information System (FIS) is foreseen in Article 11 of the Frontex Regulation.[56] It can be assumed that it is a **centralised platform** and secure communications network for exchanging information with Member States currently being developed by the agency.[57]
Purpose	Exchange of information between Frontex and Member States with a view to improving the integrated management of the external borders of the Member States of the European Union.
Personal Scope	**EU and non-EU citizens:** • persons who are subject to joint return operations; • persons who, in the context of joint operations, pilot projects and rapid interventions, are suspected, by the relevant authorities of Member States, on reasonable grounds of involvement in cross-border criminal activities, in facilitation of illegal migration activities or in human trafficking activities
Scope of information	No information available.
Size	No information available.
Retention Period	• For persons who are subject to joint return operations: **10 days maximum**. • For persons who are suspected of involvement in cross-border criminal activities, in facilitation of illegal migration activities or in human trafficking activities: **3 months maximum**.
Input	Border authorities from Member States and third countries.
Access	**Frontex**. For joint return operations: Frontex may transfer personal data to **carriers** if Member States do not transfer such data. For persons suspected of criminal activities: Frontex may transfer data to **Europol** and **other EU law enforcement agencies**.
Data Protection	**Regulation (EC) No 45/2001** applies. Processing of personal data by Frontex shall **respect the principles of necessity and proportionality** and be strictly limited to those personal data which are required for the purposes stated in the Frontex Regulation. For persons suspected of criminal activities: Frontex shall **depersonalise** the personal data used for risk-analyses. Transmission of personal data to other European Union agencies or bodies shall be subject to **specific working arrangements** regarding the exchange of personal data and subject to the prior approval of the **European Data Protection Supervisor**.

[55] Council of the EU (2004), Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25 November 2004, p. 1 (amended in 2007 and 2011).

[56] *Ibid.*

[57] Jeandesboz, Julien (2009), Police Logics and Intelligence Lead Logics in a Risk Society. Information sharing and borders: the role and limits of Frontex, Challenge Deliverable No. 264, p. 71

Costs	In its **2010** General Report, Frontex mentions delays in implementation of Frontex Information System as tendering process took more time than expected – the budget allocated to "miscellaneous operational activities" (in which FIS is included) is **550 000 Euros**.[58]
Participating States	EU-27
Involvement of EU bodies	Transmission or communication of personal data processed by Frontex to other European Union agencies or bodies requires the prior approval of the **EDPS**.

EES Entry Exit System (considered)[59]	
Type of system	The EES would involve the systematic recording of the time of entry and exit of passengers crossing the EU external borders and the provision of alerts to authorities when third country nationals overstay in the EU. **Centralised and de-centralised systems** are currently being considered.
Purpose	Dual objective for border management: **enhancing security** and **facilitating travel**.
Personal Scope	All **non-EU citizens** travelling to the EU.
Scope of information	• Alphanumeric data such as name, nationality and passport number, • Fingerprints, • Photographs, • Time, • Place of entry, • Length of authorised short stay.
Size	Should policy option of recording entries and exits of all third country nationals be pursued, **more than 350 million** (based on annual figures of international tourist arrivals in EU-27).
Retention Period	The Commission has said data could be kept in order to establish and map "travel patterns", suggesting the VIS standard of **five years** could be used.
Input	National border and visa authorities.
Access	Designated competent **visa** and **border authorities** at consular posts and at border crossing points. Also, **access to law enforcement authorities** could be envisaged in clearly defined cases and under strict rules.
Data Protection	The Commission Communication highlights Articles 7 and 8 of the Charter of Fundamental Rights, the principles of necessity in a democratic society and proportionality, the notion of "privacy by design", current EU and national legislation on data protection and supervision by the EDPS.

[58] Frontex (2011), Frontex General Report 2010, Warsaw, p. 21.

[59] European Commission (2011), Communication from the Commission to the European Parliament and the Council - Smart borders - options and the way ahead, COM(2011) 680 final, Brussels, 25 October 2011.

Costs	**623 million Euros** including a one-time development cost as well as annual costs for 5 years of operation.
Participating States	EU-27
Involvement of EU bodies	Database manager should be the **Large-scale IT Agency** in Tallinn. Data processing would be supervised by the **European Data Protection Supervisor** as far as EU institutions and bodies are involved.

RTP Registered Travellers Programme (considered)[60]	
Type of system	The RTP would allow speeding border crossing for pre-vetted travellers. The system could be a **centralised EU database** or a **de-centralised system** storing the data in "**tokens**" issued to travellers.
Purpose	To facilitate border crossings for frequent, pre-vetted and pre-screened third-country travellers at the Schengen external border; and reduce the time spent at the border crossing points.
Personal Scope	• "Bona fide" travellers: **voluntary applicants from third countries**. • **Possibly EU citizens as well** if ABC gates are rolled-out across the EU to facilitate the planned RTP (as some Member States have already introduced ABC gates to speed-up border crossings for EU citizens holding compatible passports).
Scope of information	According to the factors identified by the European Commission in 2008[61] to determine if persons are "low-risk" travellers suitable to include in an EU RTP, the following categories of data could be collected and stored: • Unique identifier to be issued to the traveller, • Alphanumerical and biometric data, including iris or face scans (already used by some Member States' RTP systems), • Frequency of travel, • Reasons for travel (business/leisure), • Reliable travel history (to check if the person respects the conditions for their length of stay on each occasion), • Proof of sufficient means of subsistence.
Size	Should policy option of recording entries and exits of all third country nationals be pursued, **more than 350 million** (based on figures of international tourist arrivals in EU- 27)
Retention Period	The Commission has said data could be kept in order to establish and map "travel patterns", suggesting the VIS standard of **five years** could be used.
Input	Border authorities

[60] Ibid.

[61] European Commission (2008), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing the next steps in border management in the European Union, COM(2008) 69 final, Brussels, 13 February 2008.

Access	Logically, **competent immigration services** and **security agencies** responsible for checking applicants against 'watch lists' should have access to the data. It is not known at this stage if law enforcement agencies will be granted routine access to RTP data.
Data Protection	The Commission Communication highlights Articles 7 and 8 of the Charter of Fundamental Rights, the principles of necessity in a democratic society and proportionality, the notion of "privacy by design", current EU and national legislation on data protection and supervision by the EDPS.
Costs	**712 million Euros** including a one-time development cost as well as annual costs for 5 years of operation.
Participating States	EU-27
Involvement of EU bodies	Database manager should be the **Large-scale IT Agency** in Tallinn. Data processing would be supervised by the **European Data Protection Supervisor.**

ABOUT CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today,
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process, and
- Provide a regular flow of authoritative publications offering policy analysis and recommendations,

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts,
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach,
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals.

Programme Structure

In-house Research Programmes

Economic and Social Welfare Policies
Financial Institutions and Markets
Energy and Climate Change
EU Foreign, Security and Neighbourhood Policy
Justice and Home Affairs
Politics and Institutions
Regulatory Affairs
Agricultural and Rural Policy

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)

Research Networks organised by CEPS

European Climate Platform (ECP)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)