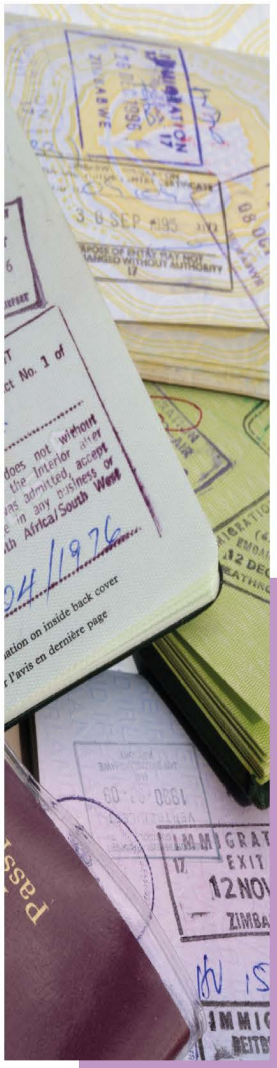
European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS



Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Smart Borders Revisited: An assessment of the Commission's revised Smart Borders proposal

STUDY FOR THE LIBE COMMITTEE

EN

2016

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Smart Borders Revisited: An assessment of the Commission's revised Smart Borders proposal

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, appraises the revised legislative proposals ('package') on EU smart borders adopted by the European Commission on 6 April 2016. It provides a general assessment of the package, focusing in particular on costs, technical feasibility and overall proportionality, and a fundamental rights check of the initiative.

PE 571.381 EN

ABOUT THE PUBLICATION

This research paper was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and was commissioned, overseen and published by the Policy Department for Citizens' Rights and Constitutional Affairs.

Policy departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.

To contact the Policy Department for Citizens' Rights and Constitutional Affairs or to subscribe to its newsletter please write to:
Poldep-citizens@ep.europa.eu

Research Administrator Responsible

Kristiina MILT
Policy Department C: Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: Poldep-citizens@ep.europa.eu

AUTHORS

Dr. Julien JEANDESBOZ, CCLS (*Centre d'étude sur les conflits*) & REPI (Université libre de Bruxelles)
Dr. Jorrit RIJPMA, Europa Institute, Leiden Law School, Leiden University
Prof. Didier BIGO, CCLS (*Centre d'étude sur les conflits*) & King's College London

The authors would like to acknowledge François Thuillier, who was consulted on law enforcement and security aspects.

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in October 2016
© European Union, 2016

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

CONTENTS

LIST OF ABBREVIATIONS

CFR	EU Charter of Fundamental Rights
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EES Regulation	Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM(2016) 194 final
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
FRA	European Union Agency for Fundamental Rights
GAMM	Global Approach to Migration Management
JHA	Justice and Home Affairs
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs of the European Parliament
NUI	National Uniform Interface
RTP	Registered Traveller Programme
SBC	Schengen Borders Code
SBC/EES Regulation	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 [Schengen Borders Code] as regards the use of the Entry/Exit System, COM(2016) 196 final
SIS (II)	Schengen Information System (Second generation)

TEU	Treaty on European Union
TFEU	Treaty on Functioning of the Europoean Union
VIS	Visa Information System
WP29	Article 29 Working Party

EXECUTIVE SUMMARY

Background

The European Commission adopted a revised legislative package for EU Smart Borders on 6 April 2016. The original Smart Borders package (which originated from two earlier Commission communications, dated February 2008 and October 2011) had been adopted in February 2013. This 2013 package was met with considerable reservations from the European Parliament and the Council, as well as the European Data Protection Supervisor (EDPS) and civil society organisations. EU Smart Borders initially included two key measures: the establishment of an Entry/Exit System (EES) and a Registered Traveller Programme (RTP) for third-country nationals crossing the EU's external borders. The 2016 revised package withdraws the legislative proposal for establishing an RTP, leaving the EES as the key feature of EU Smart Borders. EES consists of two proposed regulations: one to establish the Entry/Exit system and another to amend the Schengen Borders Code with regards to the use of the Entry/Exit system. Another key difference is law enforcement access, which the 2016 revised package foresees from the onset.

Aim

This study appraises the European Commission's revised legislative proposals for EU Smart Borders. It builds on a 2013 study "The Commission's legislative proposals on Smart Borders: their feasibility and costs" for the European Parliament that assessed the technical feasibility and cost of EU Smart Borders. The present study reviews critically the revised legislative proposals against the findings of this earlier study and concerns expressed by the European Parliament in prior reports about this initiative. The study also presents a thorough fundamental rights check.

Findings

With regard to **the review of the revised Smart Borders package in light of earlier controversies**, the study finds the following:

- The discussion on Smart Borders over the last eight years has been characterised by a regular and repeated reshuffling of objectives. The fact that the same measures are systematically put forward in **different contexts suggests that the Smart Borders measures may well not meet the general criteria of proportionality applicable to EU action**.
- The objective of better implementing EU border management policy by facilitating border-crossing procedures for third-country nationals entering or exiting the EU for the purpose of short stays has been **significantly narrowed**. With the withdrawal of RTP, **the Smart Borders package no longer creates a legal requirement for the Member States to introduce facilitation measures** (ABC gates and self-service kiosks in particular).
- The assessment work in support of the revised package is more thoroughly documented than was the case for its predecessor. Yet these **assessment efforts mostly went into demonstrating the validity of the European Commission's preferred option** rather than providing an exhaustive overview of all possible policy options.
- The **new cost** of Smart Borders to the EU budget **is EUR 480 million for four years (three years of development and deployment and one year of operation)**. This amount is lower than the EUR 623 million for five years of

development and deployment of EES in the 2013 package. In the meantime, **the accumulated cost to the EU and Member State budgets is EUR 1.013 billion for the period 2017-2026**. Furthermore, the contractor and the European Commission report **a 15-20% margin of error in costing**.

- The technical feasibility of the measures envisaged in the legislative package has been tested in real-life conditions, but the contractor, eu-LISA and the European Commission **have not delivered an implementation plan for EES**. Furthermore, **not all of the findings of the testing phase can be generalised, in particular with regard to automated/facilitation processes.**
- Overall, the measures foreseen in the Smart Borders package are, given its objectives, **disproportionate**. There is a **clear lack of evidence to confirm that EES would contribute to curbing overstaying** and **no evidence that law enforcement access to EES is relevant**. The **contribution of the envisaged measures to better implementing EU border management policy** (by reducing the workload of border guards and facilitating border crossings) **is unclear and ambiguous.**

With regard to the **fundamental rights check of the revised Smart Borders package**, the study finds the following:

- The large-scale collection and storage of personal data, including biometric data, **form an interference with the right to private life under the ECHR, and hence also under the CFR**.
- Given the special nature of biometric data, **the indiscriminate and massive collection of it makes the infringement particularly serious**.
- **The proposal fails the proportionality and necessity test** for the objectives of migration and border management as well as criminal law enforcement.

Recommendations

Regarding the **impact assessment** submitted by the European Commission:

- In light of the significant accumulated cost for the development, deployment and first seven years of operation of EES and the significant margin of error of 15-20% indicated in the costing of the proposed measures, the LIBE Committee **should require the European Commission to further clarify the financial burden and budget risk to the EU and Member States**.
- The impact assessment of the revised legislative package **does not provide a basis in evidence for the proportionality – in the sense of Article 5(4) of the TEU – of a measure that specifically aims to curb overstays of third-country nationals crossing the EU's external borders for short stays**. In this regard, the LIBE Committee should **require the European Commission to design a complementary impact study providing unambiguous evidence that the Smart Borders package does not go beyond what is necessary to achieve the objective of curbing overstaying**.
- The impact assessment of the revised legislative package **does not provide an evidence-based demonstration that law enforcement access to EES is proportionate in the sense of Article 5(4) of the TEU**. The LIBE Committee should require the European Commission, together with eu-LISA, **to provide up-to-date and detailed information regarding searches for law-enforcement**

purposes involving fingerprints in the VIS. The study finds that at this time the reporting of eu-LISA on the use of VIS for law enforcement purposes, which is used as the basis for assessing the projected use of EES, remains inconclusive, in particular for searches involving fingerprints. New evidence should be properly taken into account when considering law enforcement access to EES.

- The **additional clarifications and further evidence should be examined in a study undertaken by independent experts** before the Smart Borders package is taken into consideration by the co-legislators.

Regarding **the use of biometrics** (facial images and fingerprints) in the proposed measures:

- Although the revised legislative package constitutes an effort to minimise the biometric data collected and stored in the proposed EES, proportionality issues remain. The LIBE Committee should **consider the following options to achieve further data minimisation**.
- The **objective of replacing the physical stamping obligation can be achieved without collecting, storing or accessing fingerprints**. **It is sufficient to compare a live facial image with the facial image stored on the chip of an electronic passport to verify the identity of travellers**. This process does not require storage of facial image biometrics, thus increasing data minimisation. **Visual verification by a border guard is sufficient in cases where travellers do not carry an e-passport**. For the purpose of replacing the physical stamping obligation, the storing of data on the identity of travellers, travel document and visa information, as well as travel history for a period of 181 days is sufficient.
- Should the use of fingerprints, be considered relevant by the co-legislators, their introduction should be planned from the start to avoid issues encountered in the development of other JHA information systems. **The LIBE Committee should however consider a tiered rollout process**. To fully test the reliability of the system before particularly sensitive data is collected and stored, the introduction of fingerprints collection and storage in particular should be **made conditional upon an assessment of the functionality of EES without fingerprints after at least two years of operation**. This tiered rollout and assessment should also concern interoperability with VIS. The proposal for a regulation establishing the EES should accordingly be amended to include: 1) a **two-year moratorium on the introduction of the collection and storage of, and access to fingerprints**; 2) a **suspension clause should the functioning of EES without the collecting and storing of as well as access to fingerprints be found less than optimal**; 3) a **sunset clause foreseeing the shutdown of EES functionalities for fingerprints collection and storage** should data protection issues arise.

Regarding the **possibility of introducing further automated processes** at EU external border crossings:

- The **adoption of a harmonised legal basis for the use of automated processes for border crossings is proportionate** given the growing use by border control authorities of Member States of such processes, particularly ABC gates and e-kiosks. A harmonised legal basis **would provide legal certainty and support facilitation measures to address the growing workload of border guards at the EU's external borders**.

- As such, the proposal for a regulation to amend the Schengen Borders Code for this purpose should be considered independently from the proposal for a regulation to establish EES. **The LIBE Committee should consider the possibility of amending the proposal for a regulation to amend the Schengen Borders Code so that the provision of a harmonised legal basis for automation does not depend on the establishment of EES**.

Regarding **law enforcement access** to EES:

- At this time there is **no basis in evidence for providing law enforcement access to EES, whether by Member State authorities or Europol**. Such a measure would not meet the criteria for either necessity or proportionality, either in the sense of Article 5(4) of the TEU or interference with fundamental rights. Therefore, **the LIBE Committee should consider not endorsing law enforcement access to EES**.
- Before law enforcement access is considered, a thorough inquiry into the effective use of existing systems, especially VIS, should be conducted. At this time, the reporting of eu-LISA on the use of VIS for law enforcement purposes remains inconclusive. Since VIS has only recently completed its full rollout, a **five-year monitoring and assessment period by eu-LISA to start in 2016 or 2017 should be considered a minimum to inform a decision on law enforcement access to EES**. This would give time for law enforcement authorities in the Member States to familiarise themselves with VIS and provide information about its utility.
- Should law enforcement access to EES eventually be found relevant by the co-legislators, provisions similar to the collection and storage of biometrics should apply, namely: 1) a two-year moratorium on law enforcement access to EES in order to ensure that the system is functioning as planned; 2) a suspension clause should the functioning of EES without law enforcement access be found less than optimal; 3) a sunset clause **foreseeing the shutdown of law enforcement access to EES should it be found irrelevant (low number of searches) and/or should issues with the purpose of access or use of access arise**.

Regarding the fundamental compliance of the Smart Borders proposal with fundamental rights:

- As it stands, the EES proposal forms **a particularly serious interference with the right to respect for private life and the right to protection of personal data**. This interference should be considered **disproportionate.**
- The indiscriminate retention period of five years cannot be justified either in view of the objective of identifying overstay or for the purpose of criminal law enforcement. **The originally envisaged retention period of 181 days should be considered again.** In addition, the possibility of **distinct retention periods for distinct categories of persons** should be contemplated.
- The proposal should provide an **effective judicial remedy** for **all data subjects** in line with Article 47 CFR. This remedy should not merely cover access, correction and deletion; it also should **not be made dependent on the provision of additional personal data**.
- The transfer of data from the EES to third countries in the context of return should only be possible under the strict conditions prescribed in the proposal and **exclusively when there is an adequacy decision in the third country concerned** as regards the protection of personal data.

- The rationale for the collection and access to EES by criminal law enforcement are **not supported by objective and sound evidence**. It is the task of the EU legislator to provide such evidence.
- The proposal should **guarantee the independence of ex-ante control** of access to law enforcement.
- The provisions regulating access to the EES by law enforcement need to be drafted with much more precision so as to provide for both legal certainty and diverging approaches across the Member States. In particular: 1) in Articles 29(b) and 30(b), **the meaning of 'specific case'** should be clarified; 2) in Articles 29(b) and 29(c), **the definition of 'reasonable grounds'** should be further specified, as well as **the exact meaning of 'substantially contribute'**; 3) in Article 29, **the meaning of 'reasonable grounds' on which access to EES can be authorised without prior searches in national databases and in the Prüm system** should be clarified; 4) in Article 29, **the notion of criminal intelligence should either be defined or removed**, as it is not defined elsewhere in the EES regulation or in EU legislation and therefore constitutes too broad a criteria for authorising law enforcement access.

1. INTRODUCTION

1.1. General information and rationale of the study

This study appraises the European Commission's revised legislative proposals for EU Smart Borders. It builds on a 2013 study for the European Parliament that assessed the technical feasibility and cost of EU Smart Borders.[1] The present study reviews critically the revised legislative proposals against the findings of this earlier study and concerns expressed by the European Parliament in prior reports about this initiative. The study also presents a thorough fundamental rights check.

The original Smart Borders package (which originated from two earlier Commission communications, dated February 2008 and October 2011) was adopted by the European Commission in February 2013.[2] EU Smart Borders initially included two key measures: the establishment of an EES and a RTP for third-country nationals crossing the EU's external borders. The 2016 revised package withdraws the legislative proposal for establishing an RTP, leaving the EES as the key feature of EU Smart Borders. EES consists of two proposed regulations: one to establish the Entry/Exit system (**hereafter EES regulation**) and another to amend the Schengen Borders Code with regards to the use of the Entry/Exit system (**hereafter SBC/EES regulation**).[3]

The 2013 legislative package was poorly received. The European Parliament and the Council expressed strong reservations over its cost, technical feasibility, and scope.[4] The European Data Protection Supervisor (EDPS), the Article 29 Working Party (WP29), and civil society groups such as the Meijers Committee voiced major concerns regarding necessity and proportionality, particularly in light of the volume of personal data processing the measures would entail. The European Commission's own Impact Assessment Board twice asked DG Home to provide evidence supporting the need for EU action in relation to the objectives set by the Smart Borders package.[5]

The 2016 revised legislative package, on the other hand, is based on what the Commission has termed a 'proof-of-concept exercise'.[6] This exercise, organised in 2014-2015, comprised a technical study led by the European Commission and contracted out to PricewaterhouseCoopers (PwC), which was published, together with a report on cost analysis, in October 2014.[7] The PwC technical study outlined a series of options for implementing the Smart Borders measures, in particular the Entry-Exit System. The

[1] J. Jeandesboz, D. Bigo, B. Hayes, and S. Simon (2013), *The Commission's Legislative Proposals on Smart Borders: Their feasibility and costs*, Brussels: European Parliament, PE 462.613.
[2] European Commission (2008), *Preparing the Next Steps in Border Management in the European Union*, COM(2008) 69 final; European Commission (2011), *Smart Borders – Options and the way ahead*, COM(2011) 680 final.
[3] On EES regulation, see European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, COM(2016) 194 final. On SBC/EES regulation, see European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System*, COM(2016) 196 final.
[4] European Parliament IMPA (2013), *Initial apparaisal of a European Commission impact assessment: Smart Borders Package*, PE 514.062.
[5] European Commission Impact Assessment Board (2013), *Opinion – DG Home – Impact assessment on a proposal establishing the entry/exit system*, Brussels, 2010/HOME/004; European Commission Impact Assessment Board (2013), *Opinion – DG Home – Impact assessment on a proposal establishing the entry/exit system*, Brussels, 2010/HOME/006.
[6] European Commission (2016), *Impact Assessment Report on the establishment of an EU Entry Exit System (Part 1/3)*, Brussels, SWD(2016) 115 final, Part I, p. 1.
[7] PwC (2014), *Technical Study on Smart Borders – Final report*, Brussels: European Commission, October 2014 (hereafter referred to as *Final Report*); PwC (2014), *Technical Study on Smart Borders – Cost Analysis*, Brussels: European Commission, October 2014 (hereafter referred to as *Cost Analysis*).

options were then tested through a pilot project steered by eu-LISA, which was completed in November 2015. In the meantime, the European Commission held a series of technical and political meetings with the co-legislators and experts from the Member States; with different groups of stakeholders, including representatives from civil society, carriers and Member State law enforcement agencies; and with fundamental rights bodies, including the EDPS and the EU Fundamental Rights Agency (FRA). The LIBE Committee hosted an inter-parliamentary hearing on Smart Borders on 23 February 2015. The European Commission further opened up a public consultation on the Smart Borders package, which was published in December 2015. Along with the revised legislative package, lastly, the European Commission published a new, three-tiered impact assessment report in 2016.[8] On the basis of the 'proof-of-concept exercise' and of stakeholder mobilisation, the impact assessment report of the European Commission states that 'the question whether an Entry-Exit System is necessary and desirable is no longer in the centre of political debate. The real issue, which … forms the main part of the Impact Assessment, is *how* such a system should be developed'.[9]

1.2. General argument

The underlying assumption of the revised Smart Borders package - that the discussion on the revised package should focus exclusively on implementation - confirms one of the key observations of the 2013 study requested by the LIBE Committee. This study examined the purpose of impact assessment, finding that it presents the co-legislator with 'a set of scenarios designed to legitimise the policy option already chosen by the European Commission' rather than serving as an aid to decision-making.[10]

That the revised set of **scenarios** outlined in the 2016 Smart Borders proposals is now more strongly supported with evidence and significant stakeholder mobilisation is not in question. This observation, however, **cannot pre-empt a thorough examination of how these scenarios are now justified** (the purpose, objectives, and motivations of having EU Smart Borders) **and how these scenarios were designed** (the questions that were asked and answered through the 'proof-of-concept exercise'). A particular scenario or policy option, in other words, can be deemed feasible and financially sound, with evidence mustered to this effect, but such an assessment should not circumscribe discussions of the said scenario or policy option to a question of 'how'.

A key question here is proportionality, a constitutional principle (as per Article 5(4) of the TEU) guiding the exercise of legislative competence. At the same time, any measure that interferes with a fundamental right will need to be proportionate, which leaves the EU legislator with limited discretion only. The European Commission has organised discussions and consultations on fundamental rights issues. In the meantime, the EES foresees the systematic recording of the entries and exits of **all foreigners crossing the EU's external borders for short stays** by **collecting and storing data, including biometrics, for a five-year period**. This measure needs to be assessed against the backdrop of the European Court of Justice's rulings on other instances of systematic data collection and mass surveillance, and in particular its judgment on the Data Retention Directive on 8 April 2014.

1.3. Methodology and organisation of the study

Given the time requirements, the study is mostly based on desk research but also draws on previous research materials available to the contributors.

[8] SWD(2016) 115 final, Parts 1 to 3.
[9] SWD(2016) 115 final, Part I, p. 2, emphasis original.
[10] Jeandesboz et al., *Commission's legislative proposals*, op. cit, p. 11.

The study is organised as follows. The next section (2) reviews the 2016 Smart Borders package by providing a general assessment of the revised legislative proposals, focusing on costs, technical feasibility and overall proportionality of the initiative. The following section (3) provides a fundamental rights check of the proposals.

2. REVIEW OF THE REVISED SMART BORDERS PACKAGE

KEY FINDINGS

- The discussion on Smart Borders in the last eight years has been characterised by a regular and repeated reshuffling of objectives. The fact that the same measures should be systematically put forward in **different contexts suggests that the smart borders measures may well not meet the general criteria of proportionality applicable to EU action**.
- The objective of better implementing EU border management policy by facilitating border crossing procedures for third-country nationals entering or exiting the EU for the purpose of short stays has been **significantly narrowed**. With the withdrawal of RTP, **the Smart Borders package no longer creates a legal requirement for Member States to introduce facilitation measures** (ABC gates and self-service kiosks in particular).
- The assessment work supporting the revised package is more thoroughly documented than was the case for its predecessor. Yet these **assessment efforts mostly went into demonstrating the validity of the European Commission's preferred option** rather than providing an exhaustive overview of all possible policy options.
- The **new cost** of Smart Borders to the EU budget **is EUR 480 million for four years (three years of development and deployment and one year of operation)**. This amount is lower than the EUR 623 million for five years of development and deployment of EES in the 2013 package. In the meantime, **the accumulated cost to the EU and Member State budgets is EUR 1.013 billion for the period 2017-2026**. Furthermore, the contractor and the European Commission report **a 15-20% margin of error in costing**.
- The technical feasibility of the measures envisaged in the legislative package has been tested in real-life conditions, but the contractor, eu-LISA, and the European Commission **have not delivered an implementation plan for EES**. Furthermore, **not all of the findings of the testing phase can be generalised, in particular with regard to automated/facilitation processes**.
- Overall, the measures foreseen in the Smart Borders package are, given its objectives, **disproportionate**. There is a **clear lack of evidence to confirm that EES would contribute to curbing overstaying** and **no evidence that law enforcement access to EES is relevant**. The **contribution of the envisaged measures to better implementing EU border management policy** (by reducing the workload of border guards and facilitating border crossings) **is unclear and ambiguous.**

2.1. The outlook of the revised package

2.1.1. Scope and substance: smart borders as EES

The 2013 Smart Borders proposals comprised two key measures, the establishment of **EES** and **RTP**. The revised proposals of 2016 **only consider the establishment of EES**. The 'spirit' of RTP, nonetheless, persists with a narrower scope in the SBC/EES regulation proposal, which foresees the insertion of a new Article 8e allowing for the establishment of

optional 'national facilitation programmes' by Member State authorities (see below, section 2.1.3).

As with the earlier legislative package, the EES concerns third-country nationals who cross the EU's external borders for short stays (up to 90 days in a period of 180 days), whether they are subject to or exempt from the visa obligation. The revised EES would be a centralised system, interoperable at a central level with the Visa Information System (VIS) and with a National Uniform Interface (NUI) for communication with Member State authorities. The system would register entry and exit records for both visa-waiving and visa-holding third-country nationals. The system would process biometric data in two ways: firstly, by recording biometric identifiers from visa-waiving third country nationals (four fingerprints in combination with a facial image); secondly, by pulling biometric identifiers for visa-holding third-country nationals from VIS. The data collected in the system are retained for a five-year period. Finally, the 2016 legislative proposal, unlike its previous iteration, gives access to the EES from the onset for law enforcement authorities of the Member States and Europol.

The architecture of EES in the revised EES proposal comprises three components: a central unit, a NUI, and a connection with VIS. The central unit or system is a computerised database of biometric and alphanumeric data. EES's interoperability with VIS, which is organised at a central level, enables the pulling of biometrics (fingerprints) of Schengen visa-holding travellers from the latter system. The NUI is a single-user interface used by all Member State authorities when performing tasks linked with EES purposes.

When it comes to data subjects and data, the system **would record border crossings by all third-country nationals visiting the Schengen area for a short stay** (up to 90 days in a period of 180 days) regardless of their visa status (visa exempt, visa holders and holders of a touring visa for a duration of up to one year). **Third-country nationals who enjoy the right of free movement or the rights of free movement equivalent to those of EU citizens** (family members of EU citizens or permanent residents) **but who do not yet have a residence card are also included**.

The data registered in the EES includes 26 elements, down from 36 in the 2013 proposal:

- Identity of third-country national: first name, surname, date of birth, nationality, gender;
- Biometrics: four fingerprints and a facial image for visa-waiving third-country nationals. The EES does not store the biometric data of visa-holding persons, which remain stored in VIS;
- Information on travel document: document number, document type, document country code and expiry date;
- Information on the visa for visa-holding third-country nationals: visa sticker number, visa expiry date, number of authorised entries, authorised period of stay;
- Information on cross-border movements of the person: date and time of entry, authority allowing entry, entry border crossing point, date and time of exit, exit border crossing point;
- Information on changes of authorisation of stay: revised expiry date of the authorisation of stay, date of change of limit of stay, place of change of limit of stay, ground for change or revocation.[11]

The data retention period is five years, in contrast with the foreseen retention period of 181 days in the 2013 EES regulation.

[11] SWD(2016) 115 final, Part I, p. 34.

Finally, the **revised EES proposal provides access from the onset to Member State law enforcement services and Europol**. The initial 2013 Smart Borders proposal foresaw an evaluation of EES after two years in order to adjudicate on law enforcement access. The current proposal foresees law enforcement and Europol access 'as a secondary purpose from the start' (Chapter IV in EES regulation) 'in order to prevent, detect and investigate terrorist offences or other serious criminal offences'.[12] Law enforcement access to EES is allowed for the purposes of identification and criminal intelligence. This access, furthermore, is only granted if specific conditions are met, as specified in Articles 29 and 30 (concerning Europol) of the proposed EES regulation:

- Access is allowed if necessary 'in a specific case'.
- Access is conditioned upon the existence of 'reasonable grounds', 'in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation'.
- Access is conditioned upon unsuccessful prior searches in national databases and, in cases of fingerprint searches, upon unsuccessful prior searches in the Prüm database. Such searches are not required 'when there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject'.
- It is possible to carry out parallel requests for access to data contained in EES and VIS because only VIS stores the fingerprint data of visa-holding persons.

2.1.2. Objectives: Smart Borders as a solution in search of a problem?

The revised scope and substance of the 2016 Smart Borders legislative proposals repackage the objectives of the envisaged measures. The explanatory memorandum introducing the EES regulation lists three objectives in the following order:

- **Improving the EU's border management policy** by addressing the issue of delays at passport/immigration control and improving the quality of border checks for non-EU travellers who fall within the scope of the proposed measures. The assumption is that this can be achieved by removing the stamping obligation and by using biometrics (fingerprints and facial images), which will permit the use of automated processes such as ABC gates and self-service kiosks;
- **Improving the EU's visa and immigration policy** by providing the means, mainly through biometrics (especially fingerprints), to monitor durations of stay and the identification of persons found to have exceed their authorised stay;
- **Reinforcing the internal security of the EU and the Member States** by providing an additional identification tool (biometrics, especially fingerprints) for 'the reliable identification of terrorists, criminals, as well as of suspects and victims' and by providing the possibility to reconstruct travel histories.[13]

These objectives have, however, fluctuated over time when one considers the various iterations of the Smart Borders initiative (here in reverse chronological order):

- **The explanatory memorandum introducing the 2013 EES regulation proposal justified the measure solely on immigration policy grounds**

[12] SWD(2016) 115 final, Part I, p. 38; COM(2016) 194 final, Art. 26(1). 'Terrorist offences' are the offences under national law which correspond to or are equivalent to those referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA. 'Serious criminal offences' correspond to or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years (see Article 3(26) and 3(27) of COM(2016) 194 final).
[13] COM(2016) 194 final, pp. 2-3.

(monitoring durations of stay and taking steps against overstayers). While improving the management of EU external borders was listed as one of the expected impacts of the joint establishment of EES and RTP, **the objective of reinforcing the internal security of the EU and Member States did not feature.**[14]

- In **the 2011 Commission communication** on policy options for Smart Borders, the **primary objective was improving EU border management**, in particular the handling of increasing numbers of border crossings. This was to be accomplished by **providing support to the EU's visa policy** through monitoring durations of stay and, **as a secondary objective,** offering additional means to take steps against overstayers.[15]
- The **earliest 2008 iteration of the Smart Borders discussion** by the European Commission had **two objectives: enhancing security by intensifying the monitoring of non-EU citizens crossing the EU's external borders and facilitating the border/passport check process for what the communication labelled 'bona fide travellers'**.[16]

The discussion on Smart Borders in the last eight years **has been characterised by a regular and repeated shuffling of objectives**. While proposed legislation should logically address ongoing policy concerns, **the fact that the same measures**, albeit with some modifications, **continue to be systematically put forward in different contexts suggests that the measures do not meet the general criteria of proportionality applicable to EU action**.

2.1.3. Withdrawal of RTP: what is left of facilitation?

Facilitation has been pictured as a central issue in the various iterations of the Smart Border package. The 2008 Commission communication, 'Next steps in border management in the European Union', presented Smart Borders as a way to make '[c]rossing the external border … simple and quick for third-country nationals fulfilling the entry conditions set by Community and national law'.[17] Ensuring 'that border crossings are fast and simple for the growing number of regular travellers that constitute the vast majority of border crossers, i.e., those fulfilling all entry conditions' is foregrounded as a key challenge in the 2011 Commission communication on Smart Borders.[18] The 2016 EES proposal follows suit by identifying border check delays, along with the quality of these checks, as the first challenge to address in the establishment of Smart Borders. In the meantime, **the European Commission has withdrawn RTP from the 2016 legislative package, which suggests that the contribution of Smart Borders to facilitation has been reduced**.

First, **facilitation in the context of Smart Borders means something different than facilitation in the broader context of EU immigration and visa policies**.[19] As outlined in the Global Approach to Migration Management (GAMM), facilitation involves offering broader – and possibly fairer – possibilities of access (including with regard to the issuance of Schengen visas) to the territory of the Member States for the purposes of work, study, or travel.[20] While this definition of facilitation has been criticised for being overly instrumental and driven by security rather than labour considerations (among other concerns), it nonetheless retains a broad scope. **Facilitation is a much narrower**

[14] COM(2016) 194 final, pp. 2-3.
[15] COM(2011) 680 final, p. 2-3.
[16] COM(2008) 69 final, p. 4-5.
[17] COM(2008) 69 final, p. 2.
[18] COM(2011) 680 final, p. 3.
[19] Another meaning of facilitation, which concerns irregular migration and people smuggling, falls outside of the present discussion but has recently been scrutinised in a study commissioned on behalf of the LIBE Committee; see S. Carrera et al. (2015), *Fit for Purpose? The facilitation directive and the criminalisation of humanitarian assistance to irregular migrants*, Brussels: European Parliament, PE 536.490.
[20] European Commission (2011), *The Global Approach to Migration and Mobility*, COM(2011) 743 final.

objective in the Smart Borders package, referring to the notion that non-EU travellers should be able to clear passport and border control checks more quickly.

Concerns with faster clearance of passport and immigration checks at the EU's external borders tie in with the key justification foregrounded by the European Commission across the different communications and legislative packages on Smart Borders: namely, that the number of people crossing the EU's external borders is bound to increase significantly in the upcoming decades. **In the scenario presented by the European Commission, this expected increase in traveller numbers cannot be met by an increase in Member State personnel at external borders and thus requires a reliance on a variety of means, including automation and self-service facilities.**

The **RTP** was the core component for facilitation in the 2013 Smart Borders package. It envisaged the possibility of Schengen visa holders – provided that they submitted to a pre-vetting procedure undertaken at a consulate of one of the Member States – benefitting from facilitated checks at the EU's external borders. In the 2016 package, this measure has been **replaced in the proposed SBC/EES regulation by Articles 8c, 8d and 8e:**

- **Article 8c** permits persons whose border crossing is subject to registration in the EES to use self-service systems **to pre-enrol their individual file data in the EES**, provided that they hold a travel document with an electronic chip and that this chip contains a facial image that can be accessed by the automated system. The article further establishes that the self-service system shall verify whether the traveller has a previous registration in EES and their identity by means of a comparison between a live facial image and the facial image extracted electronically from the machine-readable zone of the passport. If this verification indicates that the traveller's data are not recorded in the EES, if the verification fails or if there are doubts as to the identity of the traveller, the self-service system shall carry out an identification using facial image and fingerprints (when and if available), including consultation of the VIS for both visa-holding and visa-exempt travellers. If the data on the person are not recorded in the EES following the identification run, or are found to require updating, the person is expected to pre-enrol with the self-service system and is then referred to a border guard.
- **Article 8d** permits persons whose border crossing is subject to a registration in EES to use self-service systems (such as kiosks) and e-gates as **de facto border checks**. To do so, the person must hold a travel document with an electronic chip containing a facial image and must be enrolled or pre-enrolled in the EES. These self-service systems and e-gates are to be monitored by a border guard.
- **Article 8e** would allow Member States to establish national facilitation programmes enabling third-country nationals to benefit from 'facilitations' when crossing the EU's external borders. National facilitation programmes can apply to all third-country nationals (whether they are obliged to hold a Schengen visa or can waive the visa obligation) or to nationals of a specific third country. For persons enrolled in national facilitation programmes, Member State authorities are allowed to derogate some of the thorough checks third-country nationals are normally subjected to, provided that a pre-vetting procedure is carried out by visa or border services. This pre-vetting procedure is largely similar to the checks carried out when issuing a Schengen visa.

In sum, and together with **Articles 8a and 8b** (which introduce the possibility for EU/EEA/CH citizens and third-country nationals holding a residence permit to use automated border control systems), the new Smart Borders package **introduces a legal basis 'foreseeing a harmonised automation of border checks for different categories of travellers'**.[21] In contrast to the 2013 legislative package, though, it does not **introduce a requirement** or **create a legal obligation** for Member State authorities

[21] COM(2016) 191 final, p. 9.

to implement such facilitation measures. This is not to say that such measures as e-gates and self-service kiosks are not already available for some categories of travellers at specific points of entry or that Member States are unlikely to introduce such measures in some cases. **The fulfilment of the facilitation objective in the current iteration of the Smart Borders package is therefore based on the assumption that such measures are introduced by Member State authorities on a widespread and systematic basis but in the absence of an obligation to do so**.

2.2. Appraisal of the impact assessment for the revised package

2.2.1. Controversies over the 2013 Smart Borders package

To what extent does the 2016 Smart Borders package (and its accompanying documentation) address the controversies triggered by its 2013 precursor? In order to appraise the 2016 package, we briefly review these earlier controversies in order to establish a baseline scenario against which potential improvements can be assessed. We focus here on issues of feasibility and cost; matters related to human rights and data protection are examined in more detail in the second half of the study. The following points are based on the 2013 study on the original Smart Borders package requested by the LIBE Committee:

- **Costs**. The 2013 package was characterised by rising costs, estimated by the European Commission at EUR 100 million in 2008 and at EUR 1.3 billion in 2011-2013. The company contracted by the European Commission in 2010 to cost the Smart Borders package indicated a 25% confidence rate for their evaluation.
- **Technical feasibility**. The 2013 study found that the original Smart Borders package did not include empirical verification of the preferred policy option. It also outlined that the European Commission and its contractors had not examined the preferred scenario for the development, deployment and operation of EU Smart Borders against experiences with likeminded systems and technologies at the Member State level and in third countries (especially the United States).

2.2.2. How the controversies were addressed: the 'proof-of-concept exercise'

The European Commission addressed the questions and controversies raised by the 2013 Smart Borders package by organising a two-step 'proof-of-concept exercise'. The current revised Smart Borders package is therefore **considerably more thoroughly documented than its predecessor**. The available documentation also provides **significantly more detail about the methodology used to calculate costs and assess technical feasibility**.

There are nonetheless **two caveats**. First, as its designation ('proof-of-concept') indicates, **the exercise was not designed to assess all possible scenarios but to demonstrate the validity of the Commission's preferred policy option against a 'no smart borders' situation**. As such, the observation that was made in relation to the impact assessment work done for the 2013 legislative package applies to the situation in 2016: namely, that **this work serves primarily as a justification for the option that the Commission has committed itself to and thus lacks independent validation**. This is all the more the case since **a number of assessment tasks (especially costing) were conducted by organisations contracted by the European Commission**. The second caveat concerns whether the significant efforts undertaken to support the current Smart Borders package should be considered as settling the question of whether Smart Borders is a desirable policy option for the EU's external borders. Here it is important to recall that the initial impact assessment supporting the 2013 package was actually found lacking by the Commission's own Impact Assessment Board and the European Parliament. **Logically, then, this is the first time that a sufficiently detailed effort at assessing the package has been undertaken.**

With these two caveats in mind, the two aspects – costing and technical feasibility – that were central to the controversies over the 2013 legislative package will be examined further. The last section (2.2.4) analyses the third component of the Smart Borders 'proof-of-concept' exercise, namely the survey conducted by the FRA with travellers on their perceptions of different components in the foreseen system (biometrics and automated gates in particular).

2.2.3. The cost of revised Smart Borders

The revised Smart Border package comes with **revised costs estimates**:

- The **cost incurred to the EU budget for three years of development** of the EES and one year of operations is estimated at **EUR 480.2 million**.
- Development costs include **EUR 222.1 million for the EES central system and NUI** and **EUR 172.67 million for thirty national EES systems** (including, for those countries that already operate an EES, the cost of integration with the NUI).
- **An additional EUR 40 million is foreseen for changes to VIS** (interoperability with VIS) **and SIS II** (the cost of creating an alert function for persons who have either not exited the EU or have not been returned at the end of the five-year data retention period in EES).
- The cost to the EU budget of **the first year of operation** of EES is estimated **to be EUR 45.47 million**, including **EUR 25.76 million for the central system** and **EUR 19.71 million for (thirty) national systems**.[22]

The new costing of Smart Borders is therefore **significantly lower** than the estimated **EUR 1.3 billion total cost** featured in the impact assessment of the 2013 package (this comparison includes **the EUR 623 million foreseen for 'EES 2013' alone**). It is also lower than the budget for Smart Borders agreed upon as part of the 2013 MFF negotiations, **set at €791 million**.

How is this revised costing achieved? First, the **decrease** in the overall costing is **due to the withdrawal of the RTP legislative proposal**. In a July 2016 briefing, DG EPRS also notes that this decrease is due to **the shortening of the system's foreseen development period** from five to three years.[23] This is confirmed in the PwC 2014 cost analysis report. Another area of cost reduction identified both in the PwC cost analysis and in the Commission impact assessment **is the shift in costs entailed by the NUI design, whereby development and deployment costs incurred by the thirty Smart Borders member states are assigned to the central level**, which reduces the complexity of coordinating thirty different development and deployment processes.[24] In the meantime, **limits and nuances to the costing analysis should be clearly pointed out**:

- First, the contractor **estimates that the cost of Smart Borders comes with a margin of error of 15-20%**.[25] Whether this is a minus or plus confidence range is not specified, but in the latter case, this means that the actual cost of Smart Borders could be between **EUR 552 million and EUR 576 million**, which is still less but closer to the cost of EES in the original package.
- Second, while the cost for development and deployment over three years and for the first year of operation has been significantly revised, it is also important to bear in mind **the cumulated cost of EES for the EU and Member State budgets in the long run**. The cost analysis included in the Commission impact assessment

[22] SWD(2016) 115 final, Part 2, pp. 65-66.
[23] EPRS (2016), *Smart Borders: EU Entry/Exit System*, Brussels: European Parliament.
[24] PwC, *Cost analysis*, op. cit., p. 9.
[25] Ibid., p. 12. At the same time, the phrasing of the cost analysis is particularly ambiguous. The cost analysis, the PwC report notes, 'assesses the cautious options … with cautious being understood as the one that would avoid underestimating the final cost' (12).

indicates that the total foreseen cumulated cost of EES over a period of 10 years would be EUR **1.013 billion**. These ten years include a three-year development period (2017-2019) and a seven-year operation period (2020-2026). It is unclear whether the 15-20% margin of error applies to this figure. Should this be the case, **the cumulated cost of developing, deploying and operating the EES could be between EUR 1.165 to 1.215 billion for the period 2017-2026**.

2.2.4. The technical feasibility of revised Smart Borders

The technical feasibility of the revised Smart Borders package has been examined in 2014-2015 through the PwC technical study and the pilot project led by eu-LISA. The technical analysis envisaged a situation where both EES and RTP would be developed and deployed. The key parameters of the technical analysis conducted by PwC and eu-LISA are as follows:

- As reported by PwC, the **technical study** mostly relied on **consultations with stakeholders** (workshops, interviews, feedback on draft deliverables), **desk research** and **on-site visits**, as well as the **results of a data collection survey** (organised by Member States in May 2014) on border crossings (numbers, types) and the categories of persons involved (EU/EEA/CH citizens, visa-exempt and visa-holding third-country nationals).[26]
- As reported by eu-LISA, the pilot project relied **on a combination of operational testing** (either in the context of the regular operations of a border crossing point or as a stand-alone process where the test was not part of regular operations) **and desk research** (literature review, interviews and workshops). The pilot project further involved consultations with stakeholders.[27]

In response to comments made on the 2013 package, then, and at least in the pilot project phase, assessment involved **testing the various options in real-life conditions** and **various contexts**. According to figures provided by eu-LISA, the tests involved 18 different border crossing point locations across 12 Member States, as well as 58 000 third-country national travellers. Furthermore, testing actually led to **discarding some options originally considered, chiefly iris enrolment**.

In the meantime, **some limits and nuances to the findings** on the technical feasibility of Smart Borders must be highlighted. First, **some aspects of technical feasibility were left out of the various studies' purview from the onset**. The PwC technical study notes that it 'does not systematically address issues related to **an implementation plan**' and only focuses in this regard on the question of whether biometrics should be introduced from the start at border checks or whether they should be deferred for the EES.[28] **In fact, the only information available about the actual implementation of the Smart Borders measures is the cost analysis**. In similar fashion, issues likely to arise on the launch of EES, such as what to do with travellers who might have crossed the EU's external borders before the rollout of the system, are not dealt with. Likewise, **eu-LISA stresses that the scope of the pilot project was limited to a subset of options outlined in the Technical Study on the basis of the Terms of Reference drafted by the European Commission**.[29] In other words, the results of the pilot **are less indicative of the feasibility of having Smart Borders than a test of the specific preferred option pursued by the European Commission**.

This observation leads to a second point, which is that **there are some gaps and leaps in logic** in the technical assessment of Smart Borders. A key example here concerns the **examination of issues related to law enforcement aspects in the PwC technical study**. The contractor, who was asked to provide a basis in evidence for law enforcement

[26] PwC, *Final Report*, op. cit., pp. 27-28.
[27] eu-LISA (2015), *Smart Borders Pilot Project – Technical Report Annexes (Volume 2)*, Tallinn: eu-LISA, pp. 12-15.
[28] PwC, *Final Report*, op. cit., p. 26.
[29] eu-LISA, *Smart Borders Pilot Project*, op. cit., p. 15.

access to Smart Border systems, **used data on law enforcement access to VIS from 1 September 2013 to 31 March 2014**.[30] The PwC technical study finds that VIS was searched for law enforcement purposes **11 times per day on average. Only five searches over the seven-month data collection period involved searches for fingerprints, and only one authentication by fingerprints occurred.** There are some mitigating factors: VIS was not fully rolled out at that stage and Member States were still in the process of deploying the organisational and technical infrastructure. The contractor nonetheless concludes **that 'it is reasonable to assume that access by law enforcement authorities to EES would remain limited, as is currently the case for VIS'**.[31] Despite this preliminary finding, however, the study then proceeds to develop a full examination of the requirements, possibilities and conditions for law enforcement access to EES. It is necessary to ask, given this observation, **whether law enforcement access to EES is actually sufficiently grounded in evidence to be implemented**, beyond the fact that it is technically feasible.

Examining the evidence basis for law enforcement access to EES requires that the most up-to-date information on law enforcement access to VIS, published by eu-LISA in its July 2016 'VIS report', is taken into consideration.[32] The VIS report covers the period from September 2013 to September 2015, and its key findings on law enforcement access can be summarised as follows[33]:

- At the time of publication, four Member States (France, Italy, Portugal, Sweden) had not yet reported their designated access points to eu-LISA;
- **By the end of the reporting period, twelve Member States did not report any activity on the use of VIS for the purpose of preventing, detecting and investigating terrorist offences and other serious criminal offences**. This group comprises Austria, Belgium, Denmark, France, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta and Slovakia. The reason (lack of reporting or no actual use) is unspecified;
- **By the end of the reporting period, eleven Member States reported a total of 9,474 searches performed by law enforcement authorities for the purpose of preventing, detecting and investigating terrorist offences and other serious criminal offences – roughly 35 searches per day**. This group includes the Czech Republic, Estonia, Finland, Germany, Greece, Hungary, the Netherlands, Poland, Slovenia, Spain and Switzerland. Out of these, three Member States reported less than 15 searches (Finland, the Netherlands, Slovenia). The largest users, according to their self-reporting, were the German (38% of the total), Hungarian (26%), Polish (14%), and Spanish (11%) authorities – **four Member States accounting for about 90% of total searches**;
- eu-LISA estimates the **total number of law enforcement users of VIS to be more than 1,200**, for **a total number of 135 access points** reported by Member States;
- The eu-LISA report **does not provide information on the volume of searches in VIS for law enforcement purposes that involved fingerprints**.

With the benefit of a longer reporting period, during which the rollout of VIS was completed, the VIS report shows that, overall, the average number of searches for law enforcement purposes in the system is **three times higher** than during the period when the PwC Technical Study on Smart Borders was realised. In the meantime, the volume of searches is **very unevenly distributed.** The authorities of **four Member States total**

[30] PwC, *Final Report*, op. cit., p. 216.
[31] PwC, *Final Report*, op. cit., p. 217.
[32] eu-LISA (2016) *VIS Report pursuant to Article 50(3) of Regulation (EC) No 767/2008 and VIS Report pursuant to Article 17(3) of Council Decision 2008/633/JHA*. Tallinn: eu-LISA, July.
[33] Ibid, pp. 23-24.

approximately 90% of reported searches, while more than half of the Member States did not report any activity. Furthermore, the VIS report does not present information on how many of the reported searches involved fingerprints. To some extent, these findings can be considered as an artefact of uneven or incomplete reporting, although this observation raises questions in itself. **It is nonetheless difficult to draw any conclusive evidence, by analogy, as to the usefulness and proportionality of law enforcement access to EES**. This is all the more the case as the depth of information and evidence available from VIS is limited at this time.

A third point concerns the **extent to which the current findings of the technical assessment of Smart Borders can be generalised**. The focus here is very much on the operational testing conducted by eu-LISA. The testing of biometric options (fingerprints, facial images, iris scans) was conducted across a variety of locations, including land and sea borders that were an area of concern in earlier controversies about the Smart Border package. Yet **the testing of ABC gates and self-service kiosks, key elements for Smart Borders achieving its objective of facilitation, has been much more limited and to some extent inconclusive**.[34] ABC gates, according to eu-LISA, were tested mainly at air borders at some of the largest EU international hubs (excluding Heathrow, United Kingdom) but only at a single sea border and only two land borders, including one train station (Gare du Nord, Paris, France). Self-service kiosks were tested at only two air borders, one sea border (Helsinki, Finland), and one land border (Sillamäe, Estonia). **For both technologies, there is a reported discrepancy in quality, duration of passage, and maturity of technology between air, land, and sea borders**. Air borders show the best results across the board, while **sea borders show the worst results for ABC gates** and **land borders the worst results for self-service kiosks**. While there are understandable limits to operational testing, it is worth noting that the use of ABC gates and self-service kiosks is a key component in the Commission's argument that Smart Borders will facilitate (in the sense of speeding up) border crossings, one of the main objectives of the package as it currently stands.

2.2.5. Travellers and Smart Borders: analysis of the results from the FRA survey

The third component in the Smart Borders 'proof-of-concept' exercise is the survey directed at third-country nationals that the FRA undertook as part of the pilot project led by eu-LISA.[35] More specifically, FRA designed to examine 'attitudes towards potential fundamental rights issues related to collecting, storing and processing biometric data in the context of border crossing'.[36] The survey also asked about specific aspects of Smart Borders that raise questions with regard to the EU Charter of Fundamental Rights, including Article 1 (dignity), Article 7 (respect for private and family life), Article 8 (right to protection of personal data), and Article 21 (non-discrimination). Fieldwork, which was contracted out to Eticas Research & Consulting, took place between 14 July 2015 and 22 October 2015; a total of 1 234 persons were interviewed.

Overall, the FRA's interpretation of the survey results is:

- that most respondents were 'comfortable' with providing biometrics at border crossing, **although 'about 30% believe that biometrics represent an interference with their private life'**. Depending on the particular biometric identifier used (iris scans triggered the strongest reaction), **'between 22% and 32% … feel that the provision of biometric data is potentially humiliating'**. In this respect, **respondents seem to consider that a check with a border guard is less humiliating than providing biometrics**;

[34] For a quick overview, see eu-LISA (2015), *Smart Borders Pilot: The results in brief*, Tallinn: eu-LISA, pp. 8-10.
[35] The report on this survey is annexed in eu-LISA, *Smart Borders Pilot Project*.
[36] eu-LISA, *Smart Borders Pilot Project*, op. cit., p. 311.

- that most respondents report 'trust in the reliability of biometric technologies'. This is mitigated by the fact that 'more than half of the respondents believe that they will not be able (or do not know if they will be able) to cross the border in case the technology does not work properly'. **Half of the respondents, furthermore, believe that it would be difficult to correct mistakes in the data**. Still on the topic of trust, the FRA reports that 'two thirds of respondents either believe that biometric technologies could harm their health or show great uncertainty on this issue'. As a final observation on trust, 'there is a widely held view that automated systems could cause less discrimination – for example on the basis of race or ethnicity – compared to checks carried out in person by border guards';
- that most respondents (80%) 'consider it important to be informed on the purpose of collecting and processing their personal data'. In particular, more than two-thirds of respondents 'would exclude children' (i.e. minors) from the obligation to provide fingerprints.[37]

The (self-reported) Commission's response to the results of the survey has been to include 'provisions for correction and redress of data to the data subjects'.[38] These, in any case, would have had to be included under EU data protection rules. For the Commission, however, the main lesson drawn is that 'the study results **confirm the acceptability of biometrics** and a wider support for fingerprints and facial image as opposed to the iris scan' (one of the technical options included for evaluation in the pilot project).[39]

A survey is notoriously difficult to implement and interpret, and for reasons of space it is not possible to question in detail respondent answers and the FRA's interpretation. It is important to note, however, that **the FRA's conclusions are more nuanced than the Commission's interpretation**. The Agency's conclusion highlights that the survey reflects 'travellers' perception' and stresses that '**violations of fundamental rights may occur regardless of whether the individual consents or not to a certain treatment, particularly in light of limited rights awareness**'.[40] In other words, **the fact that a measure or technology is acceptable to a broader or target public does not mean that it is compatible with fundamental rights and freedoms.**

'Comfort' with biometrics, furthermore, **may also be the result of limited knowledge about what the technology does and what happens to data collected this way**. When confronted with the result that a majority of respondents felt that automated systems could be less discriminatory than border guards, the Agency puts this down to a belief among respondents that 'automated systems could be programmed to identify individuals using sensitive data such as race, ethnicity or health' – which points to **the fact that respondents may well have been less than familiar with what can be done with such automated systems**.[41] This seems to be confirmed by some of the other survey results, such as views about biometrics and health or the widespread disagreement about the fingerprinting of minors. Likewise, much more could be said about the choice of phrasing the dignity-related question in terms of 'humiliation' ('Please tell use which of the following situation might be humiliating or not'). 'Humiliation' is **a very strong choice of words**: as the FRA itself notes, one could speak of an offense to dignity, a lack of respect, of being degraded, and so on. Respondents who report not feeling humiliated might still experience unease or find it disrespectful to treat travellers this way. **A more granular reading of results for this question also shows that respondents from Asia and Africa are the most likely to consider any situation involving biometrics as humiliating**, which could suggest that the degree of 'comfort' with biometrics and their impact on human dignity **might also be tied to other and more widespread**

[37] All excerpts are from eu-LISA, *Smart Borders Pilot Project*, op. cit., pp. 334-335.
[38] SWD(2016) 115 final, Part 2, p. 12.
[39] SWD(2016) 115 final, Part 2, p. 12.
[40] eu-LISA, *Smart Borders Pilot Project*, op. cit., p. 334.
[41] eu-LISA, *Smart Borders Pilot Project*, op. cit., p. 307.

experiences of racial discrimination in the European context, which could be less the case for travellers from North America and Europe.[42]

The examination of the FRA survey leads to the same observation as the one for the analysis of the assessment of the costing and technical feasibility assessment of the 2016 Smart Borders package. Since the results are ambiguous and open to interpretation, they do not constitute a compelling case supporting the policy option selected by the European Commission. Moreover, favourable public opinion towards the collection, storage and access to personal data does not in itself make these measures compliant with fundamental rights.

2.2.6. Is the revised Smart Borders package a proportionate measure?

The work done to support the revised Smart Border package gives important information on the technical feasibility of the initiative, on how sound it could be from a budget perspective, and on the attitudes of border crossers towards the technologies it would use. What remains to be discussed, however, is the extent **to which the proposed measures are proportionate: that they, in other words, do not go beyond what is necessary in terms of EU actions at the EU level to meet defined objectives**.

Proportionality with regard to fundamental rights is examined in the second part of this study. **What is examined here is proportionality in its broader sense, namely the fit between objectives and proposed measures**. The difficulty of doing so for the Smart Borders package is that **it combines three separate objectives**: improving the management of the EU's external borders (facilitation); implementing the EU's migration and visa policy (overstayers); and reinforcing internal security (law enforcement access). These three objectives are examined in turn in order to reach a general conclusion on the proportionality of the package.

The **first objective** of Smart Borders is improving the management of the EU's external borders by letting travellers, including third-country nationals, clear passport and immigration controls more quickly and lightening the workload for border guards. To recap earlier points, the proposals contribute to this objective by:

- **replacing the stamping obligation by an electronic registration of entries and exits**, thus also enabling the possibility for a prompter assessment by border guards and for better information to travellers;
- **providing a harmonised legal basis for the use of automated processes** such as ABC gates and self-service kiosks.

The impact assessment of the 2013 Smart Borders package noted likely, if minor, time gains in using EES as opposed to the status quo option, particularly upon entry.[43] The findings of the 'proof-of-concept exercise' and their summary in the impact assessment documentation accompanying the 2016 package are more elusive on these time gains. **The preferred option presented by the European Commission actually has a negative to null effect on border-crossing time** given the obligation to collect biometric data (or pull it from VIS) at first enrolment.[44] In fact, **as the conclusions of the eu-LISA pilot highlight, time gains can be expected only from the use of automated processes such as ABC gates and self-service kiosks**. The same conclusions, however, stress that **there is still a requirement for ABC gates to be supervised by a border guard**. Reliance on self-service kiosks, according to eu-LISA, would reduce border crossing times if specific conditions about where such kiosks are located can be met. In the meantime, **the use of self-service kiosks means that 'some tasks are delegated [from the border**

[42] eu-LISA, *Smart Borders Pilot Project*, op. cit., p. 322.
[43] COM(2013) 47 final, pp. 64-68.
[44] SWD(2016) 115 final, Part 1, pp. 55-59.

guard] to the traveller', which raises questions as to the actual improvement in the border crossing conditions for travellers.[45]

This calls for two remarks. First, **the use of automated processes is harmonised with the SBC/EES proposal, but there is no requirement for Member States to implement them.** Therefore, the reliance on automated processes may be likely but cannot be guaranteed. **Second, the collection and storage of fingerprints is disproportionate for the objective of replacing the stamping of passports or for enabling the use of automated processes**. These objectives can be obtained by verifying a live facial image of the traveller with the facial image contained on an electronic passport chip. Visual verification by a border guard is sufficient in cases where travellers do not carry an e-passport or when the means to verify the identity of a traveller by means of a facial image are not available. For the purpose of replacing the physical stamping obligation, the storing of data on the identity of travellers, travel document and visa information, as well as travel history for a period of 181 days is sufficient. On the other hand, the harmonised legal basis for relying on automation is proportionate given the growing reliance on ABC gates and self-service kiosks at major border-crossing points.

The **second objective** of the Smart Borders package is better implementation of the EU's migration and visa policy. The contribution of the envisaged measures **mainly deals with the issue of overstaying**. The European Commission's assumption is that EES will 'allow [authorities] to apprehend irregular migrants more efficiently', 'support the identification of irregular migrants' and in turn 'facilitate the return process'.[46]

The **proportionality of EES as a measure for dealing with overstay can be questioned** on a number of grounds. First, there is **no accurate or unambiguous data on overstay in the EU of visa-exempt and visa-holding third-country nationals currently exists**. The most recent compilation of data provided by Eurostat, from October 2015:

- shows **an increase of about 46%** in the number of non-EU citizens apprehended in relation to irregular stays between 2013 and 2014, peaking at around 626 000 persons. The Eurostat analysis notes, however, that this figure concerns apprehensions and **does not necessarily reflect a growth in the number of non-EU citizens staying irregularly** in the EU, as this change can also be linked to public policy changes in Member States;
- shows that **90% of apprehensions are recorded in ten Member States**, which can be due to gaps in reporting but also strongly suggests that this is an unevenly distributed issue;
- does not provide any information as to how many of the persons apprehended entered the EU on a short-stay Schengen visa or as visa-exempt short-stay visitors. In other words, **there is no information as to the actual scope of the overstay problem that EES sets out to address**.[47]

The second claim made in relation to the EES objective of contributing to the EU's migration policy is that it will facilitate the return process. The cost analysis attached to the Smart Borders impact assessment goes so far as to monetise the benefits of Smart Borders in this respect, foreseeing a gain for immigration services of EUR 235.3 million by operation year 7 of the EES (2026). This gain is derived from fines and a reduction in labour hours spent on identifying overstayers and implementing return decisions.[48] **This take on return policy, however, is misleading for the following reasons**:

[45] eu-LISA, *Smart Borders Pilot Project*, op. cit., pp. 163-164.
[46] COM(2016) 194 final, p. 3.
[47] Eurostat (2015), *Statistics on Enforcement of Immigration Legislation*, Luxembourg: Eurostat, available online: http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_enforcement_of_immigration_legislation#cite_ref-4 (accessed August 2016).
[48] SWD(2016) 115 final, Part 3, p. 111.

- **Available statistics** (using Eurostat reporting) show that in 2014 **only 36% of return decisions in the EU had been executed**, with about 169 000 persons returned. Between 2008 and 2014, there was a 22.1% decrease in the total number of orders to leave EU Member States. There is no single discernible reason for this trend. The identification of persons and their nationality is certainly an issue, but it is not the only one. There is also a lack of information on the proportion of return decisions concerning persons who entered the EU for a short stay. **Once again, there is no clear evidence as to the actual scope of the identification problem that EES, and especially the collection and storage of fingerprints in EES, is meant to address.**
- Return policy is regularly identified as a costly endeavour by Member States. For instance, a November 2015 report by the French Senate's Commission des Lois indicates that there is no existing assessment of the actual costs of return policy. **The cost to the budget of the French state alone, according to one 2009 evaluation, was EUR 232 million per year, which translates to EUR 12 000 per returned person.** Another assessment from 2009, which included expenses related to detention of persons in a situation of irregular stay but excluded other costs such as legal procedures, **found a total annual cost to the French budget of EUR 415.2 million**.[49]

Two conclusions emerge from this analysis. First, the assessment of the actual contribution of EES to return policy **lacks supporting evidence. There is no reliable data on the number of persons residing irregularly in the EU who entered for a short stay.** Second, the **assumption that more detections will lead to a better implementation of EU return policy (that is, Member States executing more return orders) appears to be unfounded since there is already a gap between the number of people apprehended for irregular stays and executed returns**. Finally, the notion that there would be a monetary benefit in using the EES **does not take into account the fact that a hypothetical increase in the detection of overstayers could lead to a significant increase in the workload for immigration services and courts, and therefore in spending**. As such, and as a measure to deal with overstay, the EES in its current shape cannot be considered proportionate.

The third objective of the Smart Borders package is to contribute to the internal security of the EU and the Member States by providing law enforcement and Europol access to EES. As discussed above (2.2.4), the impact assessment accompanying **the revised Smart Borders package does not provide irrefutable evidence that establishing EES with law enforcement access from the onset is proportionate with the objective of reinforcing internal security**, in particular with regard to counterterrorism and curbing serious and organised crime. In the absence of additional and more long-term data on the actual use of existing systems by Member State law enforcement agencies, in particular VIS as well as the upcoming EU Passenger Name Record (EU-PNR), **the case for law enforcement access to EES rests entirely on a measure that the EES regulation itself introduces, namely the collection and storage of biometrics (fingerprints in particular).**

There are two further points to underscore in this respect. First, **the only additional category of persons** that law enforcement agencies currently do not have access to but which they would through EES would be **visa-exempt third-country nationals entering (and exiting) the EU for short stays**. The question raised by this observation is whether the expense and effort entailed by the development, deployment, and functioning of EES is proportionate to this objective. Second, as argued in the April 2016 communication, 'Stronger and Smarter Information Systems for Border Security', **the revised Smart**

[49] Sénat, Commission des lois (2015), *Avis n°170 sur le projet de loi de finances pour 2016, TOME III: Immigration, intégration et nationalité, présenté par François-Noël Buffet*, Paris: Sénat, Session ordinaire de 2015-2016, 19 November 2015, pp. 18-19.

Border package is framed by the European Commission as part of an effort to 'join up and strengthen the EU's border management, migration and security cooperation frameworks and information tools in a comprehensive manner'.[50] The communication foresees further measures to enhance interoperability between information systems set up for law enforcement, border control, visa, and asylum purposes. A key aspect of the Commission's reasoning is that **there are data and information 'gaps'** in EU border control, in the sense that **not all persons who cross the EU's external borders have their data recorded in one way or another in EU information systems**.[51] While there are legitimate concerns as to how the complex landscape of EU information systems in the areas of freedom, security and justice can be navigated by users and data subjects alike, **collecting and storing data on all border crossers for the sake of closing 'gaps' appears to be in breach of the general principle of proportionality**, and as such cannot support the adoption of EES.[52] This is a policy issue as much as a legal matter, and in particular with regard to compliance with fundamental rights, which is examined in the next section.

[50] COM(2016) 205 final, p. 2.
[51] COM(2016) 205 final, p. 3.
[52] As demonstrated by several studies commissioned by the European Parliament and in particular the LIBE committee (see in particular D. Bigo, S. Carrera, B. Hayes, N. Hernanz, and J. Jeandesboz (2012), *Evaluating Current and Forthcoming Proposals on JHA Databases and a Smart Borders System at EU External Borders*, Brussels: European Parliament, PE 462.513).

3. COMPATIBILITY WITH FUNDAMENTAL RIGHTS

KEY FINDINGS

- The large-scale collection and storage of personal data, including biometric data, form an interference with the right to private life under the ECHR, and hence also under the CFR.
- Given the special nature of biometric data, the indiscriminate, massive collection and potential use of it constitute a particularly serious infringement.
- The proposal fails the proportionality and necessity test as it concerns both the objective of migration and border management as well as criminal law enforcement.

The main issue with regard to the compatibility with fundamental rights of the Commission's proposal for an EES relates to whether such a system would comply with Article 7 (the right to respect for private life) and Article 8 (the right to the protection of personal data) of the CFR, as interpreted by the European Court of Justice (ECJ).

3.1. Smart Borders and interference with the right to private life

3.1.1. Existence of an interference

There is no doubt that the large-scale collection and storage of personal data, including biometric data, forms an interference with the right to private life under the ECHR, and hence also under the CFR.[53]

The European Court of Human Rights (ECtHR) held that 'the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8'.[54] The subsequent use of the stored information has no bearing on that finding.[55] Rather, the access to that data by law enforcement staff forms a further interference with the right to privacy.[56] In terms of finding interference, it is irrelevant whether the information collected is sensitive or not or whether or not persons concerned have been inconvenienced in any way.[57]

In *S & Marper v the UK*, the ECtHR held that fingerprint records constitute personal data containing 'certain external identification features' comparable to photographs or voice samples.[58] They contain 'unique information about the individual concerned [sic] allowing his or her identification [to be made] with precision in a wide range of circumstances'.[59] Fingerprints, as such, belong to a special category of more sensitive data.[60] In relation to the decentralised storage of fingerprints in biometric passports, the ECJ likewise held that the processing of fingerprints constituted 'a threat' to the right to respect for private life and the right to protection of personal data, as fingerprints play an important role in the field of identifying persons in general.[61]

[53] Article 52(3) CFR.
[54] *S. and Marper v the United Kingdom* ECHR (2008) 1581, para. 67.
[55] *Amann v Switzerland* [GC], no. 27798/95, ECHR 2000-II, at para. 69, and *S. and Marper v the UK*. Cases C:465/00, C:138/01 and C:139/01, *Österreichischer Rundfunk and Others*, EU:C:2003:294, para. 75.
[56] *Leander v Sweden*, ECHR (1987), Series A, no. 116, at para. 48. Joined Cases C-293/12 (*Digital Rights Ireland*) and C-594/12 (*Kärtner Landesregierug*), EU:C:2014:238, para. 35. Hereafter referred to as *Digital Rights Ireland*.
[57] *Österreichischer Rundfunk and Others*, EU:C:2003:294, para. 75; *Digital Rights Ireland*, EU:C:2014:238, para. 33.
[58] *S. & Marper v the United Kingdom*, para. 81.
[59] *S. & Marper v the United Kingdom*, para. 84.
[60] *S. & Marper v the United Kingdom*, para. 103.
[61] *Schwarz*, EU:C:2013:670, paras. 23-30.

Given the special nature of biometric data, the indiscriminate, massive collection and potential use of it constitute a particularly serious infringement.

As the EDPS has pointed out, 'The fact that data will be retained for law enforcement purposes and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[62] The data included in the EES would not only allow for personal identification but could also help establish precise travel patterns and carry the risk of profiling on the basis of origin.

3.1.2. Justification of the interference

Under Article 8(2) of the CFR, data can only be processed with the consent of the persons concerned or if there is a legitimate basis laid down in law. **Since the EES makes the taking of fingerprints and a facial image a prerequisite for entering the Schengen area, third-country nationals are not offered a free choice, so consent cannot be considered given**.[63]

The analysis therefore shifts to the question of whether there is a legitimate basis in law for the EES. Any interference with the right to the protection of one's personal data, or right to respect for private life for that matter, must be justified under the Charter's general exception clause. **Article 52(1) of the CFR requires that any limitation is provided for by law and must respect the essence of the right. Limitations must be proportionate; they are only allowed if necessary and if they genuinely meet the objectives of a general interest recognized by the EU or the need to protect the rights of others.**

Digital Rights Ireland is the key case in which the ECJ applied Article 52(1) of the CFR to articles 7 and 8 of the CFR. The ECJ annulled the EU's Data Retention Directive for constituting a disproportionate infringement on the right to privacy and data protection.[64] This case also guides the analysis of the ECJ's Advocates General (AG) in two recent opinions on pending cases, *Tele2 Sverige AB* on national data retention laws and *Opinion 1/15* on the EU-Canada agreement on the exchange of Passenger Name Records.[65]

The EES would need to satisfy five cumulative requirements in order to justify the interference with Articles 7 and 8 of the CFR.[66] It must:

- have a legal basis;
- observe the essence of the rights enshrined in the Charter;
- genuinely pursue an objective of general interest;
- be proportionate;
- be necessary.

When it concerns the protection of personal data, the Court has moreover held that derogations and limitations cannot exceed what is *strictly* necessary.[67]

[62] G. Buttarelli (2015), 'A Data Protection perspective on the Smart Borders Package', Working Party on Frontiers, 19 November 2015.
[63] *Schwarz*, EU:C:2013:670, para. 33.
[64] *Digital Rights Ireland*, EU:C:2014:238, note 56.
[65] Opinion of AG Saugmandsgaard Øe of 19 July 2016 in Joined Cases C-203/15 *Tele2 Sverige AB v Post-och telestyrelsen* and C-698/15 *Secretary of State for Home Department v Tom Watson and Others*, EU:C:2016:572. Opinion of AG Mengozzi of 8 September 2016 on the request for an Opinion 1/15, EU:C:2016:656.
[66] *Digital Rights Ireland*, EU:C:2014:238, para. 46, with reference to the *Schecke*-test.
[67] *Digital Rights Ireland*, EU:C:2014:238, para. 46, with reference to *Institut professionnel des agents immobiliers (IPI)*, EU:C:2013:715, para. 39.

3.2. Legal basis, essence of rights and general interest

The first three requirements for a justified interference with Articles 7 and 8 of the CFR appear to be satisfied.

The EES Regulation would constitute the legal basis in law. Moreover, the proposal seems to be 'sufficiently clear and precise' in providing adequate guidance as to the circumstances and conditions under which authorities can restrict the rights at stake, thus protecting against arbitrary interference.[68] The data to be collected are clear, precise, and exhaustively listed.[69] The extent to which the proposal proves problematic in providing sufficient safeguards to effectively protect data protection rights against unlawful access and use will be discussed under the necessity requirement below.[70]

There are **no indications that the EES would affect the essence of the right to privacy or the right to personal data protection since the proposal aims to limit the amount of data collected**. It limits, for instance, the number of fingerprints when compared to the 2013 proposal; it puts in place a set of safeguards aimed at protecting personal data and privacy; and it contains provisions on the advanced deletion of data.

The EES pursues two sets of distinct objectives: one related to border and migration management and the other related to law enforcement efficacy in curbing terrorist offences and other serious criminal offences.[71] **The ECJ has recognised both aims as objectives of general interest.**[72] However, the ECJ has emphasized that an objective of general interest, no matter how fundamental, cannot in itself render a measure justified.[73]

3.3. Proportionality and necessity

Whether the EES's interference with the right to respect for private life and the right to data protection can be justified revolves around the question of whether the infringement is proportionate and necessary.

The principle of proportionality requires that acts of EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation in question and that they do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (that, in other words, no less restrictive means are available).[74] As pointed out above, the ECJ has also held that interferences with the right to data protection must not only be necessary, but *strictly* necessary.

These requirements must be considered in turn for both sets of purposes, as the collection, transfer and use of data constitute separate interferences requiring separate justifications.[75] Moreover, with the introduction of additional legal bases (Articles 87(2)(a) and 88(2)(a) TFEU), the collection of data for the objective of criminal law enforcement can no longer be considered secondary to the aim of border and migration management.

[68] AG Mengozzi in *Opinion 1/15*, EU:C:2016:65, para. 193, with reference to *Fernández Martínez v Spain*, CE:ECHR:2014:0612JUD005603007, para. 117.
[69] Articles 14-18, COM(2016) 194 final.
[70] Following the approach in *Digital Rights Ireland* rather than that of AG Mengozzi in *Opinion 1/15*.
[71] Article 5, COM(2016) 194 final.
[72] *Schwarz*, EU:C:2013:670, paras. 36-38; *Digital Rights Ireland*, EU:C:2014:238, paras. 41-44.
[73] No attention will be paid here to the Commission's reference to the refugee crisis in its impact assessment (COM(2016) 115 final, p. 2). It will be clear, however, that the changed context of the refugee crisis, which is unconnected to the scope of the EES, cannot serve in any way as to provide a legitimate objective.
[74] *Digital Rights Ireland*, EU:C:2014:238, para. 46.
[75] *Digital Rights Ireland*, EU:C:2014:238, para. 35.

3.3.1. Collection and access for the purpose of border and migration management

The objectives of the EES that can be grouped under border and migration management are enhancing the efficiency of border checks through the calculation of the period of authorised stay; identifying and detecting overstayers, both at the border and within Schengen territory; electronically register and check refusals of entry; increasing possibilities for return; enabling consulates to access information on prior travel when handling new visa requests; informing third-country nationals of the authorised duration of their stay; gathering statistics on entry and exit; and countering identity fraud. When these purposes are compared to the objectives of the 2013 proposal, it seems as if there is a stronger emphasis on the *efficiency* of border controls.[76] One new objective that has consequences for the proposed retention period involves access to the EES by consulates for the purpose of examining prior travel (in order to compensate for the removal of the entry-exit stamps in passports).[77]

3.3.1.1. Appropriateness

The EES seems to be an **appropriate tool to facilitate the work of border guards**. Entry-exit stamps may not always be legible or may be absent in the case of recently acquired passports making the calculation of authorised periods of stays more difficult. The inclusion of biometrics may further facilitate the verification of identity. In this regard the ECJ has recognised the appropriateness of the inclusion of biometric data in EU passports as a means of countering forgery, as such facilitating the work of border guards in assessing the authenticity of the document and preventing irregular migration.[78] Although the EES does not have as its purpose to combat forgery, combatting identity fraud is one of its stated purposes. The EES may also be an appropriate tool to gather statistics on exit and entry.

However, as the Article 29 Working Party and others have previously argued in relation to the 2013 proposal, the EES would only be capable of registering overstay but not locating overstayers within the Schengen area.[79] The Commission's impact assessment accompanying the 2013 proposal noted that the EES may have a deterrent effect but also conceded that it could have the effect of leading overstayers to not leave at all.[80] Moreover, it could result in irregular migrants changing strategies by opting for irregular entry rather than applying for a visa at all.[81] Finally, the mere identification of overstayers may not actually contribute to return given the very common situation in which the third country does not cooperate in return proceedings.[82]

3.3.1.2. Necessity

In relation to the purpose of gathering statistics on exit and entry, it seems difficult to maintain that the collection of personalised biometric data is necessary. As the Court held in *Watson and Belmann*, EU law does not prevent Member States from adopting measures that enable authorities to have an exact knowledge of population movements affecting their territory.[83] Since this applies to EU citizens it applies *a fortiori* to third-country nationals. That does not, however, mean that the collection and storage of individualised information

[76] Article 4, COM(2013) 95 final.
[77] Article 5(f) COM(2016) 194 final.
[78] *Schwarz*, EU:C:2013:670, para. 41.
[79] WP 29 (2013), *Opinion 05/2013 on Smart Borders*, 00952/13.
[80] Commission of the European Communities, 'Preparing the Next Steps in Border Management in the European Union – Impact Assessment', SEC(2008) 153, p. 48.
[81] S. Peers (2008), 'Proposed New EU Border Control Systems', PE 408.296, p. 9.
[82] See WP 29 (2013), *Opinion 05/2013 on Smart Borders*; Meijers Committee (2013), 'Note on the Smart Borders proposals' 3 May 2013, at *http://www.statewatch.org/news/2013/may/eu-meijers-committee-smart-borders.pdf* and EDPS (2015), 'Formal comments of the EDPS on the European Commission Public Consultation on Smart Borders', at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2015/15-11-03_Comments_smart_borders_EN.pdf.
[83] *Watson and Belmann* (1976), ECR 1185, para. 17 (EU:C:1976:106); and *Huber* (2008), ECR I-9705, para. 63 (EU:C:2008:724).

in a database is *per se* necessary, as only anonymous information is required to attain this objective.[84] Secondly, **the calculation of stay is currently done using entry-exit stamps and the Schengen calculator.** In a Presidency questionnaire, all Member States indicated that currently this is the most effective way of determining overstay, both inland and at the border.[85] **By doing away with the obligation to stamp passports upon entry and exit** – despite the fact that Member States raised concern about this abolition – **the proposal itself creates the need for a more restrictive measure**.[86] The argument that the EES will be more efficient than the stamping obligation needs to be balanced against the extent of the interference with the right to respect for private life and the protection of personal data of the EES. This is all the more so, as the proposal's abolition of entry/exit stamps has further consequences. It has created the need for consular authorities to have access to the EES in order to check the prior travel history of visa applicants.

Some elements that led the Court to annul the Data Retention Directive are also relevant for assessing the strict necessity required of the EES.

First of all, when it comes to the objective of countering overstay and irregular migration, the system covers in a generalised manner all third-country nationals entering or exiting the Union for short-stay travel without any distinction made about the potential risk of overstay. This is particularly problematic since the majority of overstayers come from countries covered by a visa obligation, which means that they can already be identified through VIS.[87] **It is difficult to maintain that the system is strictly necessary for nationals of countries not under a visa obligation. In any case, it remains unclear why the inclusion of biometric for this category of travellers would be strictly necessary as opposed to the registration of alphanumeric data.** It is relevant to recall that the Court in *Schwarz* argued that the use of biometric data in passports did not go beyond what was necessary because the data remained stored only in the passport itself and could not be used for other purposes than to prevent illegal entry, which is obviously not the case for the EES.[88] There is some disagreement as to whether *Digital Rights Ireland* should be interpreted as rendering such a generalised obligation *per se* as failing to meet the strict necessity requirement. In light of the Court's subsequent emphasis on sufficient safeguards being put in place in order to prevent unlawful access and abuse, AG Saugmandsgaard Øe does not hold that view.[89]

Second, as under the Data Retention Directive, the EES would entail automatic processing. The sheer number of authorities and consulates having access to the EES could also pose a a significant risk of unlawful access. **However, these concerns are mitigated since eu-LISA would be responsible for technical and organisational measures to achieve a high level of security; moreover, specific security rules are imposed on national authorities.** In addition, the proposal provides for supervision by the EDPS and national data protection authorities, which shall be given sufficient resources to meet that purpose. Moreover, as opposed to the Data Retention Directive, the EES proposal provides for substantive and procedural conditions relating to access to the data by the authorities as well as requirements in relation to data security.

3.3.1.3. Effective remedy

Article 46 of the EES proposal maintains the previously proposed provisions on remedies. This means that there is only the right to request access, correction or removal of data. There is no explicit remedy against incorrect data or improper use of data. Moreover, the proposal leaves it to the Member States to determine whether an action lies with a court or

[84] *Huber*, EU:C:2008:724, para. 65.
[85] Council Document 8744/15.
[86] Council Document 7592/15.
[87] See EDPS, 'Formal comments', op. cit., with reference to data provided by Frontex.
[88] *Schwarz*, EU:C:2013:670, paras. 60-62.
[89] Opinion of AG Saugmandsgaard Øe, EU:C:2016:572, paras 195-196.

with the competent authorities, which falls short of the obligation in Article 47 of the CFR to provide an effective *judicial* remedy.[90] Such a remedy is only explicitly provided for in Article 36(5) and (6) for third-country nationals who, prior to the expiry of the data retention, come to fall outside the scope of the EES (by, for instance, acquiring EU citizenship). The unqualified obligation to provide fingerprints in order to exercise the right to access, correction or deletion seems disproportionate and thus not strictly necessary.[91] Finally, the provisions on remedies do not take into sufficient account the possibility that incorrect information stored in the EES may only become apparent at the border, possibly resulting in a refusal of entry and removal. This may have far-reaching consequences for third-country nationals. It may also be difficult to effectuate the right to effective judicial protection when the third-country national is not on Member State territory.

As required by Article 47 of the CFR, the provisions on remedies should ensure effective judicial protection. The exercise of this right should not be made dependent on providing personal data and should take into account the specific situation of third-country nationals.

3.3.1.4. Retention period

The current proposal increases the retention period (originally envisaged as 180 days, the period of authorised stay) to five years.[92] We argue that this is disproportionate to the objective of determining overstay.

The Commission justifies this longer retention period:

- First by pointing to the **similar retention period in the VIS**. It is however not made clear which specific purpose the synchronizing of retention periods serves.
- Second, by pointing to the need to not disproportionately inconvenience travellers and slow down border crossing. Although these are understandable considerations, **convenience to travellers and efficiency should not be determining factors** in assessing whether a considerably longer retention period is justified in relation to the aim of determining overstay. The proposal's reasoning in recital 26 that facilitation of border crossing, for instance through self service systems "is dependent of the data registered in the system" does not explain the necessity of the five year retention period.
- Third, by pointing to **the purpose of allowing consular authorities use of the EES** for the purpose of examining a visa applicant's prior travel history, five years being the average period covered by examining entry/exit stamps.[93] Here **the need for a longer retention period is created by the proposal itself**; the new purpose to the EES is necessary because of the abolition of the duty to stamp passports on entry and exit. **Maintaining entry/exit stamps would allow for a shorter retention period while permitting consular authorities to examine a visa applicant's prior travel history**.

A five-year retention period may, in the case of a registered overstay, also result in a *de facto* entry ban, as it may prove a serious obstacle in future visa applications, especially when the overstay is negligible. Article 31(3) provides that Member States shall be informed three months prior to the expiry of the retention period. The Explanatory Memorandum explains that at the end of the data retention period an alert based on EES data can be created in the Schengen Information System (SIS). This, however, means that the data collected for the purpose of the EES is de facto prolonged. The proposal should make clear that Member States, when making an entry in the SIS using data from the EES,

[90] See also the Meijers Committee (2016), note to the Dutch Parliament on COM(2016) 194 final (in Dutch).
[91] Article 46(6), COM(2016) 194 final.
[92] Article 31, COM(2016) 195 final.
[93] The average validity of a passport is ten years. COM(2016) 115 final, 132.

are bound by the conditions of the SIS II Regulation, incuding proportionality, and thus should not do so automatically at the end of the retention period. This would avoid legal uncertainty as was observed with regard the registration of entry-bans under the Return Directive and the entry of a notification in the SIS for the purpose of refusing entry.[94]

3.3.1.5. Transfer of data to third countries

A final point of concern is the **transfer of data from the EES to third countries**. This is **in principle forbidden under Article 38 of the proposal, but an exception is made in relation to a limited set of data in the context of return proceedings**. The proposal makes this conditional on the existence of an adequacy decision or readmission agreement. **It should be made clear, however, that the existence of a readmission agreement cannot be a substitute for the existence of an adequacy decision**.[95]

3.3.2. Access to law enforcement staff for the purpose of fighting terrorism and international crime

Unlike the 2013 Proposal, the current proposal envisages access to the EES from the onset for law enforcement in order to detect, prevent, and investigate terrorist or other serious criminal offences. The EES may serve to identify or apprehend terrorists and criminal suspects (as well as identify victims) and may also serve as a criminal intelligence tool generating information on the travel histories of terrorists and criminal suspects (as well as victims). Terrorist offences and other serious criminal offences have been defined in the regulation with reference to the Framework Decision on Combatting Terrorism and the European Arrest Warrant, although the definitions provided in these measures have been criticized for a lack of specificity.[96]

3.3.2.1. Appropriateness

The ECtHR acknowledged the relevance of 'modern scientific techniques of investigation and identification' relying on certain data.[97] In relation to data retained from telecommunications, the ECJ held, in very general terms, that these may 'shed light on serious crime' and as such could from a valuable tool for criminal investigations.[98] The same could be argued for the data stored in the EES.

However, as has been repeatedly pointed out by the EDPS and others, access to personal data by law enforcement can only be allowed if the data substantially contribute to the prevention, detection or investigation of a terrorist act or criminal offence.[99] Unfortunately, such evidence is lacking from the Commission's impact assessment on the EES.

The Commission points to the VIS system, which it claims is consulted more than 14 000 times per month. The Commission also points out that law enforcement authorities have access to national entry-exit systems, which the Commission claims have 'demonstrated [to] fulfil a need'.[100] The explanatory memorandum to the proposal refers to 'cases of people who died violently and whose identification was only possible through accessing the VIS' and cases of human and drug trafficking and terrorism in which access to the VIS

[94] Meijers Committee. 2012.'Note on the coordination of the relationship between the Entry Ban and the SIS-alert: an urgent need for legislative measures'.
[95] On the importance of an adequacy decision, see *Maximillian Schrems v Data Protection Commissioner*, EU:C:2015:650.
[96] See F. Calderoni (2012), 'A Definition that Does not Work: The impact of the EU Framework Decision on the fight against organized crime', *Common Market Law Review*, vol. 49, no. 4, pp. 1365-1393, at p. 1390.
[97] *S. and Marper v the UK*, para. 105.
[98] *Digital Rights Ireland*, EU:C:2014:238, para. 49.
[99] See, for instance, EDPS, 'Formal Comments', op. cit., p. 4.
[100] COM SWD(2016) 115 final, p. 136.

allowed investigators to make 'substantial progress'. At no point, however, does the Commission present hard facts and figures that convincingly make the case for law enforcement access to the EES.

Importantly, the identification of suspects or perpetrators of serious crime or terrorist offences would merely establish their identity and presence in the Schengen area (provided that they did not cross the border irregularly). Although the mere availability of this data, in particular biometric identifiers, may assist in the context of criminal law investigations, it must be pointed out that such a 'just in case' logic justifies any mass collection of personal data, which runs counter to the principle of data minimisation.

3.3.2.2. Strict necessity

Even if one were to accept that the EES could serve as a valuable tool for criminal investigations, it must be noted again that the EES's data collection also covers people for whom there is no evidence suggesting a link with serious crime. The provisions of the EES must meet the test of strict necessity, which requires putting in place safeguards on the unlawful access and processing of data, data security, and judicial review.[101] Many of the points made in the previous section apply here *mutatis mutandis*, for which reason the following analysis will focus on those elements that are specific to the assessment of the necessity of access by law enforcement staff for the purpose of criminal law enforcement.

The EES proposal limits access in a number of ways. Article 29 stipulates that access can be necessary in a specific case when there are reasonable grounds to believe that a suspect, perpetrator or victim is covered by the scope of the EES. Access for the purpose of criminal identification - when the suspect, perpetrator or victim is unknown - is modelled on the approach taken to law enforcement access to EURODAC, that is, first requiring law enforcement to exhaust the use of existing databases and only then allowing for the search of fingerprints and facial images. Providing access to the EES for the purpose of criminal intelligence - in relation to known suspects, perpetrators or victims - would allow for the consultation of a broader data set in order to determine the travel history or periods of stay in the Schengen area.

3.3.2.3. Unclear legal drafting

The conditions and purposes of law enforcement access feature several ambiguities that deserve to be clarified in the readings of the proposed legislation by the European Parliament and the Council:

- Law enforcement access is allowed 'if necessary in a specific case' (Article 29(b) for Member State authorities and 30(b) for Europol). **The exact meaning of a 'specific case' should be defined**;
- Access is authorised if '**reasonable grounds** exist to consider that the consultation of the EES data may **substantially contribute** to the prevention, detection or investigation' of the criminal offences for which law enforcement access is envisaged in the EES regulation (Article 29(c) and 30(c)). The **only criterion for assessing what constitutes 'reasonable grounds'** is that there is 'a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation' – meaning that the suspect, perpetrator or victim is a visa-exempt third-country national (since law enforcement can access the data held in VIS for Schengen visa holders). Furthermore, the EES regulation does not establish any criteria for assessing what a 'substantial contribution' constitutes.

[101] *Digital Rights Ireland*, EU:C:2014:238, paras 57-58.

- The notion of known and unknown suspect remains undefined in the proposal, which may gave rise to differing and unnecessarily broad interpretations in different Member States.[102]
- Access to EES data is conditioned upon prior unsuccessful searches in national databases and, when the search concerns fingerprints, unsuccessful searches in the Prüm database. **However, according to Article 29 of the EES regulation, such prior searches are not required** 'when there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject'. **This is extremely ambiguous since there is no definition here of what constitutes 'reasonable grounds'**. The question here is **how such reasonable grounds for not performing prior searches can be established in the absence of said prior searches.**
- The purpose of law enforcement access to EES is repeatedly presented as 'criminal identification'. Article 29 of the EES regulation, however, also opens up the possibility of 'access to the EES as a criminal intelligence tool'. **Criminal intelligence, however, is not defined in EU legislation; for its part, the regulation does not include a definition**. Criminal intelligence is therefore **a broad, unsubstantiated motive for law enforcement access to EES, requiring either clarification or removal**.

3.3.2.4. Ex-ante review

The ECJ in *Digital Rights Ireland* made clear that access by law enforcement requires prior review by a court or independent administrative body.[103] This court or independent administrative body should, upon a reasoned request by the authorities, assess whether access is strictly necessary for the purpose of the objective pursued. The EES proposal requires that Member States designate one (or more) central access points to verify reasoned request for access by law enforcement authorities. Article 26(3) of the proposal, however, allows the central access point to be part of a law enforcement authority. Although it stresses that the central access point should act independently, this cannot guarantee its full independence.[104]

3.3.2.5. Retention period

A final concern regards the necessity of the proposed five-year retention period. No distinction is made in terms of the retention period as regards people who may be linked to terrorism or serious organised crime and those who are not. Such distinction should of course be made on objective factors and not profiling. Moreover, as regard to the length of the retention period, one can consider the opinion of AG Cruz-Villalón in *Digital Rights Ireland*: 'without denying that there are criminal activities which are prepared well in advance, I have not found … any sufficient justification for not limiting the data retention period to be established by the Member States to less than one year'.[105]

The justification brought forward by the Commission in its impact assessment is based on the average period during which law enforcement staff in the Member States have had most recourse to national entry-exit systems, after which a rapid decline of consultations could be observed.[106] Again, however, the mere fact that consultations take place and the frequency with which they are carried out does not in itself say anything about the necessity of a five-year retention period. The alignment of retention periods with those of other databases (EURODAC, VIS) may be attractive in its simplicity but cannot itself justify a five-year retention period.

[102] See also the Meijers Committee, note to the Dutch Parliament, op. cit.
[103] *Digital Rights Ireland*, EU:C:2014:238, para. 62.
[104] On the importance of the independence of supervisory authorities, see *Commission v Germany*, EU:C:2010:125, para. 25.
[105] Opinion of AG Cruz Villalón of 11 December 2013 in *Digital Rights Ireland*, EU:C:2013:845, para. 149.
[106] COM(2016) 115 final, p. 137.

The five-year retention period must be considered as disproportionately long. At a minimum, a distinction should be made regarding the data of third-country nationals who have been linked to terrorism or serious organised crime and those who have not.

Only to the extent that overstay could be linked, on the basis of solid evidence, to serious organised crime and terrorist activity should overstay be taken into account.

3.4. Final considerations: evidence base and interoperability

The Commission has gone to great lengths to bring its proposal for an EES in line with the requirements of EU data protection law and ECJ case law. There are, however, a number of concerns that remain and which seem to be in contradiction with the ECJ's ruling in *Digital Rights Ireland*.

There is no solid evidence for the necessity of large-scale and indiscriminate storage of personal data, both **in relation to the system's objective of border and migration management as well as access by law enforcement.** In addition, **the five-year retention period** under the new proposal **is unjustifiably long.** There is **no guaranteed independence of the central access point exercising an ex-ante review of the necessity of access by law enforcement authorities.**

Some further general comments are in order at this point. Even if the EES were to be found in full compliance with data protection legislation, the system cannot be considered in isolation. Rather, it forms part of an ever-expanding infrastructure of systems aimed at regulating borders, migration and asylum as well as fighting against terrorism and organised crime (SIS II, VIS, EURODAC, PNR, API). Although the 2004 Hague Programme stipulated that new centralised European databases should only be created on the basis of studies that show their added value, in the past decade there has been little restraint in the establishment of new databases as well as the expansion of the scope of existing ones.[107] A thorough evaluation of the use of the databases, in particular as regards the access of law enforcement staff, should therefore be considered before setting up a new system. As the EDPS quite accurately pointed out, the key challenge is to balance a legal framework for data protection based on the minimisation of data collection with the belief in the benefits of big data.[108]

Working in synergy with each other, these justice and home affairs databases may form a surveillance architecture that may not be desirable in a liberal democracy. It may be questioned to what extent the current legal framework for the protection of the right to private life and the right to personal data may be capable of addressing such concerns.

Interoperability, which is foreseen in the proposal between the VIS and the EES, does not in itself constitute an interference with the rights laid down in Article 7 and 8 of the CFR, as long as the principle of purpose limitation is respected.[109] There is, of course, a danger that this principle can be effectively sidelined when new purposes are added to existing legal bases.[110] Moreover, as the EDPS cautioned, **the proliferation of databases and the fact that they run on interoperable technical platforms may form 'a powerful drive only for the *de facto* accession or exchange**

[107] The Hague Programme, Annex to the European Council Conclusions, Brussels, 4-5 November 2004, point 2.1, at europa.eu/rapid/press-release_DOC-04-5_en.doc.
[108] Buttarelli, 'A Data Protection Perspective', op. cit.
[109] One inconsistency needs to be pointed out here, namely that the new EES proposal provides for operability to minimise the inconvenience caused by having to collect fingerprints yet at the same time adds a facial image to the data collection and does not make it available in the VIS.
[110] See V. Mitsilegas (2005), 'Contrôle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme', *Cultures & Conflits*, no. 58, pp. 185-197.

of data'.[111] This is particularly true when the same authorities have access to different databases. At the regulatory level as well, the mere existence of the technological possibility may inform policy choices rather than the other way round.[112] It is telling in this regard that the Bratislava Declaration and Road Map in the formal European Council on 16 September 2016 expressly referred to the need for 'interconnected' databases at the EU's external borders.

[111] EDPS (2006), *Comments on the Communication of the Commission on interoperability of European databases*, at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf.
[112] J. Huysmans (2006), *The Politics of Insecurity: Fear, migration and asylum in the EU*, London: Routledge, pp. 8-9.

4. RECOMMENDATIONS

It follows from the key findings of the study that the outcome of the 2014-2015 'proof-of-concept exercise' is the **first thorough documentation of the policy option favoured by the European Commission rather than a demonstration of the budgetary soundness, technical feasibility, proportionality and compliance with fundamental rights of the proposed measures**.

4.1. Assessment of the revised Smart Borders package

Regarding the impact assessment submitted by the European Commission:

- In light of the significant accumulated cost for the development, deployment and first seven years of operation of EES and the significant margin of error of 15-20% indicated in the costing of the proposed measures, the LIBE Committee **should require the European Commission to further clarify the financial burden and budget risk to the EU and Member States**.
- The impact assessment of the revised legislative package **does not provide a basis in evidence for the proportionality – in the sense of Article 5(4) of the TEU – of a measure that specifically aims to curb overstays of third-country nationals crossing the EU's external borders for short stays**. In this regard, the LIBE Committee should **require the European Commission to design a complementary impact study providing unambiguous evidence that the Smart Borders package does not go beyond what is necessary to achieve the objective of curbing overstaying**.
- The impact assessment of the revised legislative package **does not provide an evidence-based demonstration that law enforcement access to EES is proportionate in the sense of Article 5(4) of the TEU**. The LIBE Committee should require the European Commission, together with eu-LISA, **to provide up-to-date and detailed information regarding searches for law-enforcement purposes involving fingerprints in the VIS**. The study finds that at this time the **reporting of eu-LISA on the use of VIS for law enforcement purposes**, which is used as the basis for assessing the projected use of EES, **remains inconclusive, in particular for searches involving fingerprints**. New evidence should be properly taken into account when considering law enforcement access to EES.
- The **additional clarifications and further evidence should be examined in a study undertaken by independent experts** before the Smart Borders legislative package is taken into consideration by the co-legislators.

4.2. Biometrics

Regarding the use of biometrics (facial images and biometrics) in the proposed measures:

- Although the revised legislative package constitutes an effort to minimise the biometric data collected and stored in the proposed EES, proportionality issues remain. The LIBE Committee should **consider the following options to achieve further data minimisation**.
- The **objective of replacing the physical stamping obligation can be achieved without collecting, storing or accessing fingerprints**. **It is sufficient to compare a live facial image with the facial image stored on the chip of an electronic passport to verify the identity of travellers**. This process does not require storage of facial image biometrics, thus increasing data minimisation. **Visual verification by a border guard is sufficient in cases where travellers do not**

carry an e-passport. For the purpose of replacing the physical stamping obligation, the storing of data on the identity of travellers, travel document and visa information, as well as travel history for a period of 181 days is sufficient.

- Should the use of fingerprints, be considered relevant by the co-legislators, their introduction should be planned from the start to avoid issues encountered in the development of other JHA information systems. **The LIBE Committee should however consider a tiered rollout process**. To fully test the reliability of the system before particularly sensitive data is collected and stored, the introduction of fingerprints collection and storage in particular should be **made conditional upon an assessment of the functionality of EES without fingerprints after at least two years of operation**. This tiered rollout and assessment should also concern interoperability with VIS. The proposal for a regulation establishing the EES should accordingly be amended to include: 1) a **two-year moratorium on the introduction of the collection and storage of, and access to fingerprints**; 2) a **suspension clause should the functioning of EES without the collecting and storing of as well as access to fingerprints be found less than optimal**; 3) a **sunset clause foreseeing the shutdown of EES functionalities for fingerprints collection and storage** should data protection issues arise.

4.3. Automation of border checks

Regarding the possibility of introducing further automated processes at EU external border crossings:

- The **adoption of a harmonised legal basis for the use of automated processes for border crossings is proportionate** given the growing use by border control authorities of Member States of such processes, particularly ABC gates and e-kiosks. A harmonised legal basis **would provide legal certainty and support facilitation measures to address the growing workload of border guards at the EU's external borders**.
- As such, the proposal for a regulation to amend the Schengen Borders Code for this purpose should be considered independently from the proposal for a regulation to establish EES. **The LIBE Committee should consider the possibility of amending the proposal for a regulation to amend the Schengen Borders Code so that the provision of a harmonised legal basis for automation does not depend on the establishment of EES**.

4.4. Law enforcement access

Regarding law enforcement access to EES:

- At this time there is **no basis in evidence for providing law enforcement access to EES, whether by Member State authorities or Europol**. Such a measure would not meet the criteria for either necessity or proportionality, either in the sense of Article 5(4) of the TEU or interference with fundamental rights. Therefore, **the LIBE Committee should consider not endorsing law enforcement access to EES**.
- Before law enforcement access is considered, a thorough inquiry into the effective use of existing systems, especially VIS, should be conducted. At this time, the reporting of eu-LISA on the use of VIS for law enforcement purposes remains inconclusive. Since VIS has only recently completed its full rollout, a **five-year monitoring and assessment period by eu-LISA to start in 2016 or 2017**

should be considered a minimum to inform a decision on law enforcement access to EES. This would give time for law enforcement authorities in the Member States to familiarise themselves with VIS and provide information about its utility.

- Should law enforcement access to EES eventually be found relevant by the co-legislators, provisions similar to the collection and storage of biometrics should apply, namely: 1) a two-year moratorium on law enforcement access to EES in order to ensure that the system is functioning as planned; 2) a suspension clause should the functioning of EES without law enforcement access be found less than optimal; 3) a sunset clause **foreseeing the shutdown of law enforcement access to EES should it be found irrelevant (low number of searches) and/or should issues with the purpose of access or use of access arise**.

4.5. Fundamental rights compliance

In addition to the recommendations made in relation to the use of biometrics under the proportionality assessment under Article 5(4) of the TEU, the following recommendations can be made in relation to the fundamental compliance of the Smart Borders proposal with fundamental rights:

- As it stands, the EES proposal forms **a particularly serious interference with the right to respect for private life and the right to protection of personal data**. This interference should be considered **disproportionate.**
- The indiscriminate retention period of five years cannot be justified either in view of the objective of identifying overstay or for the purpose of criminal law enforcement. **The originally envisaged retention period of 181 days should be considered again.** In addition, the possibility of **distinct retention periods for distinct categories of persons** should be contemplated.
- The proposal should provide an **effective judicial remedy** for **all data subjects** in line with Article 47 CFR. This remedy should not merely cover access, correction and deletion; it also should **not be made dependent on the provision of additional personal data**.
- The transfer of data from the EES to third countries in the context of return should only be possible under the strict conditions prescribed in the proposal and **exclusively when there is an adequacy decision in the third country concerned** as regards the protection of personal data.
- The rationale for the collection and access to EES by criminal law enforcement are **not supported by objective and sound evidence**. It is the task of the EU legislator to provide such evidence.
- The proposal should **guarantee the independence of ex-ante control** of access to law enforcement.
- The provisions regulating access to the EES by law enforcement need to be drafted with much more precision so as to provide for both legal certainty and diverging approaches across the Member States. In particular: 1) in Articles 29(b) and 30(b), **the meaning of 'specific case'** should be clarified; 2) in Articles 29(b) and 29(c), **the definition of 'reasonable grounds'** should be further specified, as well as **the exact meaning of 'substantially contribute'**; 3) in Article 29, **the meaning of 'reasonable grounds' on which access to EES can be authorised without prior searches in national databases and in the Prüm system** should be clarified; 4) in Article 29, **the notion of criminal intelligence should either be defined or removed**, as it is not defined elsewhere in the EES regulation or in EU legislation and therefore constitutes too broad a criteria for authorising law enforcement access.

REFERENCES

Case Law

- *Amann v Switzerland* [GC], no. 27798/95, ECHR 2000-II.
- *Commission v Germany*, EU:C:2010:125.
- *Digital Rights Ireland*, EU:C:2014:238 (judgment) and EU:C:2013:845 (opinion).
- *Fernández Martínez v Spain*, CE:ECHR:2014:0612.
- *Huber*, EU:C:2008:724.
- *Institut professionnel des agents immobiliers (IPI)*, EU:C:2013:715.
- *Leander v Sweden*, ECHR (1987), Series A, no. 116.
- *Maximillian Schrems v Data Protection Commissioner*, EU:C:2015:650.
- *Opinion 1/15*, EU:C:2016:656.
- *Österreichischer Rundfunk and Others*, EU:C:2003:294.
- *S. and Marper v the United Kingdom* ECHR (2008) 1581.
- *Schwarz*, EU:C:2013:670.
- *Tele2Sverige* (Opinion), EU:C:2016:572.
- *Watson and Belmann*, EU:C:1976:106.

Policy and Secondary Sources

- Bigo, D., S. Carrera, B. Hayes, N. Hernanz, and J. Jeandesboz. 2012. *Evaluating Current and Forthcoming Proposals on JHA Databases and a Smart Borders System at EU External Borders*. Brussels: European Parliament. PE 462.513.
- Buttarelli, G. 2015. 'A Data Protection perspective on the Smart Borders Package'. Working Party on Frontiers.
- Calderoni, F. 2012. 'A Definition that Does not Work: The impact of the EU Framework Decision on the fight against organized crime'. *Common Market Law Review*, vol. 49, no. 4, pp. 1365-1393.
- Carrera, S. et al. 2015. *Fit for Purpose? The facilitation directive and the criminalisation of humanitarian assistance to irregular migrants*. Brussels: European Parliament. PE 536.490.
- Commission of the European Communities. 'Preparing the Next Steps in Border Management in the European Union – Impact Assessment'. SEC(2008) 153.

- European Parliamentary Research Service. 2016. *Smart Borders: EU Entry/Exit System*. Brussels: European Parliament.
- eu-LISA. 2015. *Smart Borders Pilot: The results in brief*. Tallinn: eu-LISA.
- eu-LISA. 2015. *Smart Borders Pilot Project – Technical Report Annexes (Volume 2)*. Tallinn: eu-LISA.
- eu-LISA (2016) *VIS Report pursuant to Article 50(3) of Regulation (EC) No 767/2008 and VIS Report pursuant to Article 17(3) of Council Decision 2008/633/JHA*. Tallinn: eu-LISA.
- European Commission. 2016. *Impact Assessment Report on the establishment of an EU Entry Exit System (Part 1/3)*. SWD(2016) 115 final.
- European Commission. 2016. *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System*. COM(2016) 196 final.
- European Commission. 2016. *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*. COM(2016) 194 final.
- European Commission Impact Assessment Board. 2013. *Opinion – DG Home – Impact assessment on a proposal establishing the entry/exit system*. 2010/HOME/004.
- European Commission Impact Assessment Board. 2013. *Opinion – DG Home – Impact assessment on a proposal establishing the entry/exit system*, Brussels. 2010/HOME/006.
- European Commission. 2011. *The Global Approach to Migration and Mobility*. COM(2011) 743 final.
- European Commission. 2011. *Smart Borders – Options and the way ahead*. COM(2011) 680 final.
- European Commission. 2008. *Preparing the Next Steps in Border Management in the European Union*. COM(2008) 69 final.
- European Data Protection Supervisor. 2015. 'Formal comments of the EDPS on the European Commission Public Consultation on Smart Borders'. Available online: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2015/15-11-03_Comments_smart_borders_EN.pdf.
- European Data Protection Supervisor. 2006. *Comments on the Communication of the Commission on interoperability of European databases*. Available online: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf.
- Eurostat. 2015. *Statistics on Enforcement of Immigration Legislation*. Luxembourg: Eurostat. Available online: http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_enforcement_of_immigration_legislation#cite_ref-4.

- The Hague Programme. Annex to the European Council Conclusions. Brussels, 4-5 November 2004. Available online: europa.eu/rapid/press-release_DOC-04-5_en.doc.
- Huysmans, J. 2006. *The Politics of Insecurity: Fear, migration and asylum in the EU*. London: Routledge.
- Jeandesboz, J., D. Bigo, B. Hayes, and S. Simon. 2013. *The Commission's Legislative Proposals on Smart Borders: Their feasibility and costs*. Brussels: European Parliament. PE 462.613.
- Meijers Committee. 2012.'Note on the coordination of the relationship between the Entry Ban and the SIS- alert: an urgent need for legislative measures'.
- Meijers Committee. 2013. 'Note on the Smart Borders proposals'.
- Meijers Committee. 2016. Note to the Dutch Parliament on COM(2016) 194 final.
- Mitsilegas, V. 2005. 'Contrôle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme'. *Cultures & Conflits*, no. 58, pp. 185-197.
- Peers, S. 2008. 'Proposed New EU Border Control Systems'. PE 408.296.
- PricewaterhouseCoopers. 2014. *Technical Study on Smart Borders – Cost Analysis*. Brussels: European Commission.
- PricewaterhouseCoopers. 2014. *Technical Study on Smart Borders – Final report*. Brussels: European Commission.
- Sénat, Commission des lois. 2015. *Avis n°170 sur le projet de loi de finances pour 2016, TOME III: Immigration, intégration et nationalité, présenté par François-Noël Buffet*. Paris: Sénat, Session ordinaire de 2015-2016, 19 November 2015.
- Working Party 29. 2013. *Opinion 05/2013 on Smart Borders*. 00952/13.

CAT: QA-06-16-165-EN-C (paper)
CAT: QA-06-16-165-EN-N (pdf)

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

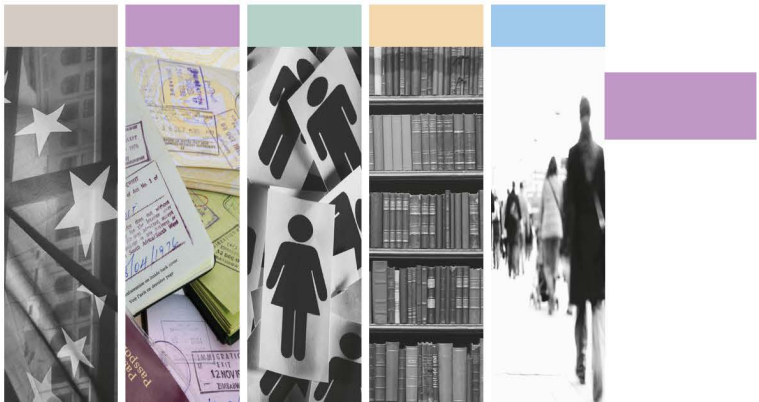
Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT: iStock International Inc.



ISBN 978-92-846-0182-0 (paper)
ISBN 978-92-846-0183-7 (pdf)

doi: 10.2861/660969 (paper)
doi: 10.2861/189840 (pdf)

Publications Office