Immigration and Privacy in the Law of the EU: 
The Case of Databases

Niovi Vavoula

Submitted in fulfillment of the requirements of the Degree of Doctor of 
Philosophy - Ph.D. (Laws)

Supervisors: Prof. Valsamis Mitsilegas and Prof. Elspeth Guild
I, Niovi Vavoula, confirm that the research included within this thesis is my own work or that where it has been carried out in collaboration with, or supported by others, that this is duly acknowledged below and my contribution indicated. Previously published material is also acknowledged below.

I attest that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge break any UK law, infringe any third party’s copyright or other Intellectual Property Right, or contain any confidential material.

I accept that the College has the right to use plagiarism detection software to check the electronic version of the thesis.

I confirm that this thesis has not been previously submitted for the award of a degree by this or any other university.

The copyright of this thesis rests with the author and no quotation from it or information derived from it may be published without the prior written consent of the author.

Signature: Niovi Vavoula

3 October 2016
Abstract

The past three decades have been marked by the proliferation of highly sophisticated pan-European databases processing a wide range of personal data collected by different categories of third-country nationals. At present, three databases are fully operational: the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac, which largely target ‘unwanted’ irregular migrants, visa applicants and applicants for international protection respectively. The momentum for immigration databases is currently high, as in addition to significant reforms to the legal regime of the existing schemes, the EU legislator envisages the setting up of an Entry/Exit System, as well as databases for residence permits, long-stay visas and travel authorisations. This thesis examines the privacy concerns raised by the establishment and operation of EU immigration databases. Rather than viewing information processing through the lens of EU data protection law, it is argued that the right to private life, as enshrined in Articles 7 EUCFR and 8 ECHR, provides more holistic protection to individuals. In this context, this thesis provides a typology of standards for compliance with privacy on the basis of the jurisprudence of the ECtHR and CJEU. Having set the theoretical foundations of the study, the legal framework of the aforementioned information systems is analysed and evaluated in light of the right to private life. It is submitted that the collection and further processing of everyday personal information and biometric data -which are sensitive in nature- constitutes a disproportionate form of surveillance of movement, which allows constructing profiles of third-country nationals, recreating their travel routes and eventually deterring and obstructing their mobility. Law enforcement access to these systems constitutes a separate limitation to privacy, which, albeit not taking place on a routine basis, poses grave proportionality concerns.
Acknowledgements

Although a Ph.D. thesis carries the single name of the researcher on the cover, the process of its completion is always accomplished through the combined help and support of other people. Therefore, I would like to hereby acknowledge my appreciation to all the actors who contributed to the completion of this thesis. Firstly, I would like to express my deepest gratitude to my Ph.D. supervisors, Professor Valsamis Mitsilegas and Professor Elspeth Guild. I have been privileged to work with two highly knowledgeable academics who have enthusiastically embraced the researched topic and have equally contributed to the realisation of this project. Their constant encouragement, constructive comments and patience throughout the years are priceless. I am very much indebted to Professor Mitsilegas not only for helping me to gain confidence in my work, but also for his kind generosity, not least for giving me the opportunity to be employed at QMUL as his Research Assistant. Professor Guild’s continuous support and insightful suggestions have been a major motivation and have helped me tremendously in ‘thinking outside of the box’. Secondly, I am very grateful to the Immigration Law Practitioners’ Association (ILPA) and the Department of Law of QMUL for providing funding to my research. It would be impossible to pursue my doctoral studies if it had not been for this financial support. Thirdly, I would also like to thank several colleagues and academics that have taken interest in my research. The European Criminal Law Academic Network (ECLAN), through its Ph.D. seminars, has given me the chance to test my arguments and receive valuable feedback. Concerning my research stay in Brussels, I am indebted to Professor Anne Weyembergh, who generously allowed me to be affiliated with ULB, to Emilio de Capitani, for providing me help and guidance to navigate myself in the EU institutions and to all Officers in Brussels and Athens who have kindly agreed to devote their time to discuss my thesis. I am also very grateful to my colleagues not only at QMUL, but also in other institutions, whose kind words have been very reassuring and comforting. I hope I have made my gratitude known to them already. My friends in London, particularly Elena, Metka and Amir, deserve special thanks for their support, both practical and emotional. As for my friends in Athens, I wholeheartedly thank them for their love and encouragement all these years. Elena, Giota, Vassiliki, Marianna, Vera, Antonis and Loukas have always been very supportive and have helped me much more than they think. My greatest thanks go to my mother, Angeliki, for believing in me and for standing by me through every step not only of the thesis, but also of my life. This thesis is partly dedicated to her as the smallest sign of my gratitude.
To my mother, who is always there for me and to the loving memory of my father.
Abbreviations

ADIS  Arrival and Departure Information System
AFIS  Automated Fingerprint Identification System
AFSJ  Area of Freedom, Security and Justice
CEAS  Common European Asylum System
CISA  Convention Implementing the Schengen Agreement
CJEU  Court of Justice of the European Union
C.SIS  Central Schengen Information System
CS.SIS  Central Schengen Information System II
C-VIS  Central Visa Information System
DG    Directorate General
DHS   Department of Homeland Security
DPA   Data Protection Authority
DPWP  Data Protection Working Party
EASO  European Asylum Support Office
EAW   European Arrest Warrant
EC    European Community
ECHR  European Convention on Human Rights
ECJ   European Court of Justice
ECRE  European Council on Refugees and Exiles
ECTHR European Court of Human Rights
EDPS  European Data Protection Supervisor
EES   Entry/Exit System
EHRR  European Human Rights Reports
EMN   European Migration Network
EP    European Parliament
EPIC  Electronic Privacy Information Center
ESTA  Electronic System of Travel Authorisation
ETIAS European Travel Information and Authorisation System
EUCFR European Union Charter of Fundamental Rights
Eurodac European Dactyloscopy
Eurosur European External Border Surveillance System
EU    European Union
cu-LISA EU for the operational management of large-scale IT systems in the AFSJ
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAR</td>
<td>False Acceptance Rate</td>
</tr>
<tr>
<td>FRA</td>
<td>Fundamental Rights Agency</td>
</tr>
<tr>
<td>FRONTEX</td>
<td>EU for the Management of Operational Cooperation at the External Borders</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
</tr>
<tr>
<td>FTE</td>
<td>Failure to Enroll</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant of Civil and Political Rights</td>
</tr>
<tr>
<td>IDENT</td>
<td>Automated Biometric Identification System</td>
</tr>
<tr>
<td>IOM</td>
<td>International Organisation for Migration</td>
</tr>
<tr>
<td>JHA</td>
<td>Justice and Home Affairs</td>
</tr>
<tr>
<td>JSA</td>
<td>Joint Supervisory Authority</td>
</tr>
<tr>
<td>JSB</td>
<td>Joint Supervisory Body (Europol)</td>
</tr>
<tr>
<td>MEP</td>
<td>Member of the European Parliament</td>
</tr>
<tr>
<td>NEES</td>
<td>National Entry Exit System</td>
</tr>
<tr>
<td>NI-SIS</td>
<td>National Interfaces – Schengen Information System</td>
</tr>
<tr>
<td>NSEER</td>
<td>National Security Entry-Exit Registration</td>
</tr>
<tr>
<td>N.SIS</td>
<td>National Schengen Information System</td>
</tr>
<tr>
<td>N.SIS II</td>
<td>National Schengen Information System II</td>
</tr>
<tr>
<td>N-VIS</td>
<td>National Visa Information System</td>
</tr>
<tr>
<td>OBIM</td>
<td>Office of Biometric Identity Management</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Records</td>
</tr>
<tr>
<td>RTP</td>
<td>Registered Traveller Programme</td>
</tr>
<tr>
<td>SBC</td>
<td>Schengen Borders Code</td>
</tr>
<tr>
<td>SIRENE</td>
<td>Supplementary Information Request at the National Entries</td>
</tr>
<tr>
<td>SIS</td>
<td>Schengen Information System</td>
</tr>
<tr>
<td>SIS II</td>
<td>Second generation Schengen Information System</td>
</tr>
<tr>
<td>TEC</td>
<td>Treaty of the European Community</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty of the European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>UDHR</td>
<td>Universal Declaration of Human Rights</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UNHCR</td>
<td>United Nations High Commissioner for Refugees</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>US-VISIT</td>
<td>United States Visitor and Immigration Status Indicator Technology</td>
</tr>
</tbody>
</table>
Contents

Abstract .............................................................................................................................................3
Acknowledgements ..............................................................................................................................4
Abbreviations .....................................................................................................................................6
Contents ................................................................................................................................................8
Introduction .........................................................................................................................................16
  1. Subject matter and aim ..................................................................................................................16
  2. Limitations ......................................................................................................................................21
  3. Sources ..........................................................................................................................................22
  4. Terminology ....................................................................................................................................23
  5. Arrangement of chapters ................................................................................................................25
CHAPTER 1. Unravelling Ariandne’s Thread: Data Processing and Privacy in the EU Legal Order .........................................................................................................................27
  1. Introduction ....................................................................................................................................27
  2. Conceptualising privacy ..................................................................................................................28
  3. The protection of privacy under EU law ........................................................................................32
    3.1 Sources .......................................................................................................................................32
    3.2 The constitutional protection of privacy and the genesis of Article 8 EUCFR ....................35
      3.2.1 Introducing the ‘right to respect for private life’ (Article 7 EUCFR) ............................35
      3.2.2 Introducing the ‘right to the protection of personal data’ (Article 8 EUCFR) ..........37
    3.3 Privacy and data protection – ‘Dangerous liaisons’? .............................................................39
    3.4 The ‘anatomy’ of the right to the protection of personal data – Conceptual ambiguities leading to inherent limitations ........................................................................................................41
      3.4.1 Ambiguities stemming from the wording of Article 8 EUCFR ....................................41
        a) The ‘prohibitive’ approach .................................................................................................41
        b) The ‘permissive’ approach .............................................................................................42
      3.4.2 ‘Deconstructing’ the right to the protection of personal data – Privacy as providing more holistic protection ........................................................................................................................................44
4. Judicial assessment of privacy: The jurisprudence of the ECtHR as a source for inspiration.................................................................47

4.1 Introducing ‘the right to respect for private life’ (Article 8 ECHR) ............47

4.2 The ECtHR on the definition of privacy: Endorsing constructive flexibility .....49

4.3 The processing of personal data as an aspect of private life .........................51

4.4 Determination of interference under Article 8(1) ECHR ...............................53

4.5 Justification of interference under Article 8(2) ECHR .................................57

4.5.1 The ‘in accordance with law’ requirement...................................................57

4.5.2 The existence of a legitimate aim.................................................................59

4.5.3 The proportionality test ..............................................................................59

5. Judicial assessment of privacy: The CJEU as the ‘unlikely hero of data privacy in Europe’ ........................................................................................................63

5.1 The interplay between data protection and privacy – Conceptual clarifications and the centrality of privacy ........................................................................63

5.1.1 Pre-Lisbon ................................................................................................63

5.1.2 Post-Lisbon ................................................................................................64

5.2 Key characteristics of privacy protection ................................................................68

5.2.1 The judgment in Schwarz – Problematising the storage of fingerprint data ...68

   a) Legal and factual background ..................................................................68

   b) The Court’s ruling ...............................................................................68

5.2.2 The judgment in Digital Rights Ireland – ‘A new hope’ for privacy ............71

   a) Legal and factual background ..................................................................71

   b) The Court’s ruling ...............................................................................73

   c) Post-Digital Rights Ireland: Privacy and pre-emptive surveillance ..........78

5.2.3 The judgment in Schrems – From the ‘Safe Harbor’ back into the (data transfer) storm ..................................................................................82

   a) Legal and factual background ..................................................................82

   b) The Court’s ruling ...............................................................................83

6. Conclusion ...........................................................................................................86

CHAPTER 2. The ‘Success Story’ of the Schengen Information System (SIS): A Reporting System Transformed into an Investigatory Tool.................................92
1. Introduction ............................................................................................................................... 92
2. Schengen cooperation in a nutshell .......................................................................................... 93
3. The Schengen Information System (SIS) .................................................................................. 95
   3.1 Step one: The establishment of the SIS .............................................................................. 95
       3.1.1 Introduction to the SIS .............................................................................................. 95
       3.1.2 Alerts on third-country nationals: Keeping away the ‘unwanted’ .............................. 97
3.2 Step two: The reinvigoration of the SIS in the aftermath of 9/11 ...................................... 100
       3.2.1 Thinking ‘outside of the box’ - Far-reaching suggestions by Member States 100
       3.2.2 The Spanish initiative ............................................................................................... 101
4. The second generation Schengen Information System (SIS II) ............................................. 103
   4.1 Step three: The set up of the SIS II ................................................................................... 103
       4.1.1 The long and winding road to the SIS II ................................................................... 103
       4.1.2 Introduction to the SIS II .......................................................................................... 105
       4.1.3 Overview of the SIS II Regulation ............................................................................ 107
           a) Scope and purpose ........................................................................................................ 107
           b) Categories of registered data ....................................................................................... 108
           c) Substantive grounds for a listing in the SIS II .............................................................. 110
               i) The ‘usual suspects’ .................................................................................................. 110
               ii) Beneficiaries of EU law ......................................................................................... 114
               iii) The ‘banned’ ........................................................................................................... 114
           d) Retention period ........................................................................................................... 115
           e) Access to the data ........................................................................................................ 116
           f) Interlinking of alerts ..................................................................................................... 118
           g) Individual rights ........................................................................................................... 119
           h) Supervision .................................................................................................................. 120
   4.2 Step four: Additional features in response to the phenomenon of ‘foreign fighters’ .......... 120
5. Evaluation of the SIS II in light of Article 7 EUCFR .............................................................. 121
   5.1 Application of Article 7 EUCFR ......................................................................................... 121
   5.2 Essence of privacy ............................................................................................................. 122
   5.3 Objective of general interest ............................................................................................. 122
5.4 Is the limitation ‘provided for by law’? ................................................................. 123
5.5 Proportionality test ......................................................................................... 124
  5.5.1 Personal scope ............................................................................................ 124
  5.5.2 Inclusion of biometrics .............................................................................. 128
  5.5.3 Retention period ....................................................................................... 131
  5.5.4 Accessing authorities ................................................................................ 132
  5.5.5 Interlinking of alerts .................................................................................. 133
6. Conclusion ........................................................................................................ 134

CHAPTER 3. The Establishment of the Visa Information System (VIS): A Decisive
Step towards Surveillance of Movement ................................................................. 137

  1. Introduction ........................................................................................................ 137
  2. An outline of the EU common policy on short-term visas ......................... 138
  3. The Visa Information System (VIS): A multifunctional tool ..................... 141
    3.1 A long history in short .................................................................................. 141
    3.2 VIS Regulation ............................................................................................ 144
      3.2.1 Introduction to the VIS .......................................................................... 144
      3.2.2 The ‘umbrella’ purpose of the VIS and the case C-482/08 UK v Council .... 146
      3.2.2 Categories of data .................................................................................. 148
      3.2.3 Retention period .................................................................................... 151
      3.2.4 Accessing authorities ............................................................................. 152
      3.2.5 Transfer of data ..................................................................................... 153
      3.2.6 Individual rights .................................................................................... 154
      3.2.7 Supervision ............................................................................................. 155
      3.2.8 ‘Bridging’ clause ................................................................................... 155
    3.3 VIS Decision .................................................................................................. 156
      3.3.1 Authorities ............................................................................................... 158
      3.3.2 Procedure ............................................................................................... 159
      3.3.3 Conditions ............................................................................................... 159
### 3.3.4 Transfer of data

- Evaluation of the VIS in light of Article 7 EUCFR
- Application of Article 7 EUCFR
- Essence of privacy
- Objective of general interest
- Is the limitation ‘provided for by law’?
- Proportionality of the VIS as an immigration and asylum tool

### 4. Evaluation of the VIS in light of Article 7 EUCFR

- Application of Article 7 EUCFR
- Essence of privacy
- Objective of general interest
- Is the limitation ‘provided for by law’?
- Proportionality of the VIS as an immigration and asylum tool

### 5. Conclusion

#### CHAPTER 4. The Tale of Eurodac – An ‘Ugly Duckling’ Turning into a Swan?

1. Introduction
2. We need to talk about...Dublin
3. Eurodac: The ‘truth serum’ of the EU asylum policy
   - The early days
   - The Eurodac Regulation
   - Law enforcement access to Eurodac data: A record-breaking issue
   - The recast Eurodac Regulation
   - Operation of Eurodac as an asylum tool
   - Consultation by law enforcement authorities and Europol
     - Authorities involved
     - Procedure
     - Conditions of access
     - Transfer of data
     - Latent fingerprints
3.5 Eurodac under pressure – The massive influx of refugees and migrants...........201
3.6 The 2016 Commission proposal........................................................................202
4. Evaluation of Eurodac in light of Article 7 EUCFR...........................................205
4.1 Assessing the establishment of Eurodac as a tool to facilitate the Dublin mechanism...........................................................................................................205
4.1.1 Application of Article 7 EUCFR......................................................................205
4.1.2 Essence of privacy............................................................................................206
4.1.3 Objective of general interest.............................................................................206
4.1.4 Is the limitation ‘provided for by law’?..............................................................207
4.1.5 Proportionality test..........................................................................................207
4.2 Assessing the comparison of Eurodac data for law enforcement purposes ......212
4.2.1 Law enforcement access: A separate limitation to privacy with far reaching consequences.....................................................................................................................212
4.2.2 Necessity of law enforcement access - flawed design of national databases or a flawed perception of asylum seekers?.................................................................213
4.2.3 Proportionality of law enforcement access.......................................................217
4.3 Assessing the re-package of Eurodac as an instrument for ‘wider immigration purposes’ .................................................................................................................................220
5. Conclusion.............................................................................................................223

CHAPTER 5. ‘Mind the (Information) Gap’: The Normalisation of Surveillance of Movement via the Entry/Exit System (EES).........................................................226
1. Introduction............................................................................................................226
2. The story behind the EES proposals.......................................................................227
2.1 ‘Born in the USA’: The origins of the EES.........................................................227
2.2 From the VIS to the EES....................................................................................231
3. Towards the establishment of a ‘Schengen Hotel’: Mapping the Commission proposals..........................................................................................................................235
3.1 The proposal of 2013............................................................................................235
3.1.1 Main characteristics of the proposed EES.......................................................235
3.1.2 The ‘elephant in the room’: Law enforcement access to EES data............................................................................. 237
3.2 The proposal of 2016 .......................................................................................................................................................... 239
3.2.1 Purpose ........................................................................................................................................................................ 240
3.2.2 Personal scope ............................................................................................................................................................... 241
3.2.3 Enrolment in the EES and use of collected data ........................................................................................................... 243
3.2.4 Law enforcement access .................................................................................................................................................. 244
3.2.5 Other provisions ............................................................................................................................................................. 246
4. Evaluation of the EES in light of Article 7 EUCFR ........................................................................................................... 247
4.1 Application of Article 7 EUCFR ........................................................................................................................................ 247
4.2 Essence of privacy ............................................................................................................................................................... 249
4.3 Objective of general interest ................................................................................................................................................ 249
4.4 Is the limitation ‘provided for by law’? ............................................................................................................................ 249
4.5 Proportionality test ............................................................................................................................................................ 250
4.5.1 Proportionality of the EES as an immigration control tool ......................................................................................... 251
4.5.2 Proportionality of the EES as a law enforcement tool ................................................................................................. 257
5. Conclusion ............................................................................................................................................................................. 261

CHAPTER 6. ‘The Shape of Things to Come’: EU Immigration Databases in Transition ........................................................................ 263

1. Introduction ........................................................................................................................................................................ 263
2. The Registered Traveller Programme (RTP): The ‘good’, the ‘bad’ and the ‘ugly’ travellers ............................................. 264
2.1 Background information ..................................................................................................................................................... 264
2.2 Overview of the proposal ................................................................................................................................................... 265
2.3 Evaluation of the RTP in light of Article 7 EUCFR ........................................................................................................... 269
3. European Travel Information and Authorisation System (ETIAS): A flanking measure of the EU’s visa policy 272
4. Holders of residence permits, residence cards and long-stay visas: Next in line? 274
5. Interoperability ................................................................................................................................................................. 275
6. Conclusion ............................................................................................................................................................................. 277
Introduction

'Databases certainly present a privacy problem, but what exactly is the nature of that problem?'.

1. Subject matter and aim

The past three decades have witnessed a profound transformation in the way immigration control is performed at EU level. The traditional model, whereby entry decisions are taken at the border crossing points and national authorities tackle irregular migration both at external borders and on national territory, has been progressively reinforced with strategies that move action outside and beyond the physical border.² This extraterritorialisation is inextricably linked with a shift in focus; the object of control is no longer solely the border, but emphasis is placed on how to deter the flow of migrants before they reach the EU territory and deflect responsibility.³ Border control is evolving into migration flow management in an ongoing process of identifying and preventing ‘risky’ elements.⁴ A dominant feature of modern immigration control is the growing intertwining of immigration with security. This link has been highlighted already since the mid-1990s when Bigo noted the development of an (in)security continuum that supplies the field of migration with security concerns related to crime control.⁵ Under the influence of terrorist events in the US, Madrid and London, the process of securitising migration took a negative turn. In response to the attacks, and to a large extent under the influence of similar developments in the US, the EU expressly established a nexus between immigration control and counter-terrorism.⁶

2 For an analysis see Bernard Ryan and Valsamis Mitsilegas (eds), Extraterritorial Immigration Control (Martinus Nijhoff 2010).
visa applications, as well as entry and exit procedures, were put under the microscope, as they were also deemed important for the prevention and investigation of crimes, particularly terrorism.\footnote{The Hague Programme mentions that ‘the management of migration flows, including the fight against illegal immigration, should be strengthened by establishing a continuum of security measures that effectively links visa application procedures and entry and exit procedures at external border crossings. Such measures are also of importance for the prevention and control of crime, in particular terrorism’. See The Hague Programme: Strengthening Freedom, Security and Justice in the European Union [2004] OJ C53/1, 7.} As Mitsilegas has eloquently pointed out, securitisation has thus deepened by taking place in a two-fold manner; on the one hand through the use of immigration control instruments to pursue criminal law objectives, and on the other hand by employing security methods in order to conduct border and immigration controls.\footnote{Valsamis Mitsilegas, The Criminalisation of Migration in Europe – Challenges for Human Rights and the Rule of Law (Springer 2015) 29.}

The rapid technological evolution has been an indispensable component of these efforts to acquire – or regain – control over the movement of third-country nationals.\footnote{The terminology depends on whether one may argue that governments have lost control of immigration or that managing migration has been a very powerful myth. For the respective views see respectively Saskia Sassen, Losing Control? Sovereignty in an Age of Globalization (Columbia University Press 1998); Elspeth Guild and Didier Bigo, ‘The Transformation of European Border Controls’ in Bernard Ryan and Valsamis Mitsilegas (eds), Extraterritorial Immigration Control (n2).} Technology has been the ‘servant mistress of politics’\footnote{Philippe Bonditti, ‘From Territorial Spaces to Networks: A Foucaultian Approach to the Implementation of Biometry’ (2004) 29 Alternatives: Global, Local, Political 465.} and has significantly upgraded the methods through which immigration control is performed, leading to what Besters and Brom term as ‘the digitalisation of the European migration policy’.\footnote{Michiel Besters and Frans Brom, “Greedy” Information Technology: The Digitalization of the European Migration Policy’ (2010) 12(4) European Journal of Migration and Law 455.} In this framework, modern technological advents, particularly the most controversial ones such as fingerprinting, ‘terrorist profiling’ and travel surveillance, ‘have been (and are still being) "tested" on migrants and refugees or otherwise legitimized at the border’.\footnote{Ben Hayes, NeoConOpticon: The EU Security-Industrial Complex (Transnational Institute/Statewatch 2009) 35. See Katja Lindskov Jacobsen, ‘Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation’ (2010) 14(1) Citizenship Studies 89.} Biometry in particular has been championed as a tool that can be deployed to reliably determine whether a third-country national is who he claims he is.\footnote{For a thorough analysis on biometrics see Els Kindt, Privacy and Data Protection Issues of Biometric Identifiers (Springer 2013).} The preference on identifying individuals using their biological characteristics is attributed to a number of qualities that they carry, such as their universality, distinctiveness and permanence.\footnote{Anil Jain, Ruud Bolle and Sharath Pankanti, Personal Identification in Networked Society (Kluwer 1999). For an analysis on implementing biometrics at the borders see Commission, ‘Biometrics at the frontiers: Assessing the impact on society’ (2005).} Their introduction creates an ‘anchor’ for identity in the human body, to which
information can be fixed, resulting in its ‘informatisation’. Furthermore, to picture the new state of affairs, scholars have described borders as ‘digital’ and ‘biometric’. However, reliance on technological tools has been criticised as based on an ‘untested belief’ that they will offer the ultimate solution to any threat the EU may face, and security considerations superseding individual rights. In this respect, concerns have been voiced on multiple grounds; reliability of biometric data, association with criminality and loss of dignity, ethical and societal implications.

The present thesis lies at the crossroads of the aforementioned trends. Facilitated by the evolution of digital technologies, and to a large extent driven by security considerations in the post-9/11 world, the EU legislator has established highly sophisticated centralised databases that store and further process a wide range of personal data collected from different groups of third-country nationals. Currently, a multi-layered network has been constructed comprising of three operational databases: the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac. In a nutshell, the SIS II is the updated version of the SIS, which was the first Schengen-wide system partly implemented for the purpose of controlling the migration flow. Mixed in nature and security oriented, the SIS II contains inter alia information in the form of ‘alerts’ on ‘unwanted aliens’ based either on public policy, public security, or national security grounds, or on breaches of domestic immigration law. The VIS functions as a multi-purpose tool registering personal data of short-stay visitors subject to visa requirements. Eurodac, in its current form, records the fingerprints of asylum seekers as well as some categories of irregular migrants. The momentum for EU immigration databases is currently higher than ever. In addition to consecutive enhancements of the aforementioned systems spanning from modest ‘corrective’ additions to radical reforms, EU centralised systems are bound to proliferate. The entry and exit of visa exempt tourists will be monitored through the proposed Entry/Exit System (EES). Furthermore, these visitors will have to obtain

---

16 Irma van der Ploeg, ‘Biometric Identification Technologies: Ethical Implications of the Informatization of the Body’ (No 1, Biometric Technology & Ethics 2005); Annemarie Sprokkereef and Paul De Hert, ‘Ethical Practice in the Use of Biometric Identifiers within the EU’ (2007) 3 Law, Science and Policy 177.
authorisation to travel by pre-registering relevant information regarding their intended journey. Frequent travellers may enjoy facilitated border crossing via the Registered Traveller Programme (RTP) in exchange for voluntarily disclosing their personal information and successfully going through extensive background checks. Finally, personal data of long-stay visa holders and holders of residence permits may also be collected and centrally stored in the future.

The EU legislator is essentially establishing a ‘millefeuille’ of information processing schemes based on routinely collecting various types of personal data from third-country nationals, including biometrics, primarily for administrative purposes, but which may also be processed by authorities responsible for law enforcement. As such, immigration control has progressively acquired characteristics of mass surveillance of movement, whereby different groups of third-country nationals are classified according to the dangers they pose to society and surveillance techniques become the vehicle for managing their risk. As Gammeltoft-Hansen eloquently observes, EU immigration databases form part of concentric ‘risk filters’ serving to categorise and identify migrants. In this context, Broeders has framed immigration databases as forming part of the ‘panoptic Europe’, an ever-growing strategy designed to exclude third-country nationals through delegitimisation and criminalisation. Bigo instead coins the term ‘banopticon’ in order to highlight the fact that these systems are not intended for monitoring everybody, but rather target the immediately designated risk groups only, constituting an exclusionary form of control with a focus on banishment and prevention or denying entry.

24 Gammeltoft-Hansen (n4) 8.
EU immigration databases constitute a central cog in the EU information collection machine,27 exemplified also by the setting up of a specialised EU Agency entrusted with their management, eu-LISA.28 However, their setting up and operation pose grave challenges to fundamental rights, particularly to the right to private life (Articles 7 EUCFR and 8 ECHR) and the right to the protection of personal data (Article 8 EUCFR). Over time, such challenges have been in the spotlight of several legal scholars. In particular, Kabera Karanja thoroughly analyses the SIS in terms of privacy and data protection,29 whereas Brouwer examines the right to effective remedies by third-country nationals who have been reported in the SIS.30 Within this framework, her study discusses how this right is depicted and protected under privacy and data protection law, and examines relevant case law particularly of the ECtHR. Furthermore, Tzanou discusses in one of her case studies in her Ph.D. thesis data protection issues raised specifically by the consultation of EU immigration databases for law enforcement purposes.31 Boehm follows a similar approach when examining more generally the information exchange schemes in the AFSJ, but she additionally examines access to immigration databases by Europol.32 Additionally, Mitsilegas has repeatedly emphasised the importance of privacy protection when assessing information exchange systems and has correctly placed the set up of databases within the general framework of criminalising migration, highlighting the nexus between crime prevention and immigration control.33

In light of the above, the aim of the present thesis is to analyse the privacy concerns raised by the establishment and operation of EU large-scale information systems that store and further process personal data collected from different groups of third-country nationals. Rather than anchoring the fundamental rights challenges posed by databases to data protection law only, this thesis calls for the centrality of privacy, taking the view that this right provides a more holistic protection to third-country nationals without, however, negating the importance of data protection law. Therefore,

30 Brouwer, *Digital Borders and Real Rights* (n17).
33 Valsamis Mitsilegas, *The Criminalisation of Migration in Europe* (n8) 29-42.
whilst the main research question tackled by this thesis relates to the impact of the operation of databases upon the privacy of third-country nationals whose personal data are stored therein, the nature of the relationship between the two rights necessarily falls within the realms of the analysis. Furthermore, it must be pointed out that whereas certain privacy concerns have been touched upon by other scholars, there is no comprehensive, systematic and up-to-date analysis as to how exactly the right to private life is affected. It is acknowledged that all EU immigration databases carry various common characteristics, such as the requirement of collecting and processing biometric data. However, this thesis starts from the premise that due to the differentiated legal regime afforded by the EU legislator, and the overall compartmentalised approach of the EU in this respect, an examination of each system on its own merit is essential.

2. Limitations

Of course this study has its limitations through its research design. Firstly, it does not address all EU immigration control instruments that involve the processing of personal data, but it only focuses on pan-European, large-scale information systems, both operational and on paper. Consequently, other personal data processing instruments enacted for the purposes of immigration control, or with quasi-immigration control effects, such as the Eurosur Regulation\textsuperscript{34} or the EU PNR Directive,\textsuperscript{35} do not fall within the auspices of this thesis. A further limitation relates to the case of the SIS II, which, as noted earlier, comprises of two branches. In view of the researched topic, this thesis necessarily examines the immigration aspects of the database, even though the criminal law branch may contain ‘alerts’ on third-country nationals. Accordingly, the rules on that branch of the SIS II pursuing policing purposes are not thoroughly discussed, although some important differences between the two instruments are highlighted.\textsuperscript{36} Thirdly, it must be noted that the perspective of this thesis is EU fundamental rights law. Therefore, aspects related to information technology law, such


\textsuperscript{36} For an analysis on the features of the SIS II Decision see Tzanou (n31) 157-88.
as data security of the systems, are outside the remit of this thesis. The final, but no less important, limitation of this study is *ratione temporis*. I have been fortunate enough to conduct this research during a very ‘fertile’ period for EU immigration databases. However, in light of phenomena such as the massive influx of refugees and migrants in the EU, or the alleged proliferation of ‘foreign fighters’, the momentum for upgrading operational schemes or developing new ones is currently high. Additional functionalities will soon be proposed in relation to the SIS II and the modalities of law enforcement access to VIS and Eurodac data may be revised. The Eurodac database is under ‘refurbishment’ on the basis of a Commission proposal, whereas the EES is on the negotiating table and the RTP is temporarily put on ice. Finally, discussion on possible interconnection among the different schemes has recently gained fresh impetus. Further developments are still to appear, but the present research necessarily describes the situation as it exists up to 31st July 2016.

3. Sources

The research mainly employs EU legal documents. The analysis of EU primary law and secondary legislation such as Regulations, Directives, Council Decisions and Framework Decisions are at the heart of this thesis, as are rulings of the CJEU and the ECtHR. Due attention is being paid to the views expressed by relevant EU stakeholders, such as the EDPS. The position of the Parliament is reflected in Reports and Working Documents, whereas the Commission’s various Reports, Working Documents, Impact Assessments and Communications are advisory. Reports by eu-LISA are central for shedding light into the practical operation of immigration databases. Council documents constitute an important part of the research; their consultation is vital in order to map not only the desires and concerns as expressed by EU Member States, but also the extent to which these have been integrated into the final text. On numerous occasions, Council documents were not publicly accessible. In those cases where Statewatch had not published the documents in question online, it has been necessary to request access by the General Secretariat of the Council. However, certain documents that reveal

---

37 For a general overview see Bart Justers and others (eds), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases* (Springer 2013).
38 The EDPS’ general objective is to ensure that the European institutions and bodies respect the right to privacy when they process personal data and develop new policies.
39 Around 60 documents have been requested, the vast majority of which were disclosed (48).
domestic border control policies or national law enforcement practices, or that involve discussions that are still ongoing at the time of writing were not disclosed. Where appropriate, US sources, particularly Government Accountability Reports (GAO), are consulted, without the aim of adding a comparative dimension to this study.

Furthermore, in order to gain valuable insights into the different approaches among the EU institutions and agencies, it was decided to conduct informal discussion with relevant EU stakeholders. Each discussion took place on the basis of a set of questions sent to them prior to the appointment or call. The questions were tailor-made depending on the position of the discussant and their expertise, and the specific topic of discussion. The format of anonymous informal discussions is preferred, as opposed to fully-structured interviews, to allow stakeholders to speak more freely. These took place in Brussels during November and December 2014. The discussants were: three Officers from the EPDS; two MEPs who were Rapporteurs in relevant legislative proposals; one Officer from the Secretariat of the LIBE Committee; five Officers from the DG Home; and one Officer from eu-LISA. Where appropriate, their input is inserted into this thesis, but it must be pointed out that since the conduct of the discussions a number of issues changed, therefore their replies have not always been relevant. In addition, in August 2014, I had an informal discussion with an Officer at the Greek Ministry of Interior regarding the operation of the SIS II.

Privacy, data protection and immigration control are fields that have generated an abundant amount of literature, mainly coming from legal scholars, political scientists, sociologists and information scientists. The legal scholarship, books, articles, commentaries, case notes, policy briefs and reports are valuable sources of the present thesis. It goes without saying that a selection process is inevitable. As a result, those pieces of research that are most closely related to the aim of this thesis have been preferred.

4. Terminology

Due to the rather technical nature of the topic under research (at least to a certain extent), this thesis uses numerous terms that require further explanation.

‘Privacy’ is understood as the ‘right to respect for private life’ as referred to in Articles 8 ECHR and 7 EUCFR. Although Chapter 1 is devoted to the examination of this right, I must clarify at this point the following: González Fuster has thoroughly
mapped the ‘convoluted relations’ between the different terms of ‘privacy’ and ‘private life’ in international law, which, as Bygrave notes, derive from ‘terminological idiosyncrasies’ at the domestic level. On the one hand it is observed that the ECtHR has over time resisted the use of the term ‘privacy’ when referring to Article 8 ECHR, and has privileged instead the notion of ‘respect to private life’. On the other hand, EU secondary law regards Article 8 ECHR as establishing a right to privacy, a term also commonly referred to by the CJEU. Whist taking note of this terminological ‘cocktail’, in line with the EU approach, the aforementioned terms are configured as equivalent, and are, thus, used interchangeably.

‘Personal data’ are to be understood as any information related to an identified, or identifiable, natural person. Often the thesis uses the terms ‘information’ or ‘personal information’ instead of the more accurate ‘personal data’. Nevertheless, for the purposes of the present analysis both terms should be viewed as synonymous.

‘Processing’ means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. When a distinction between the collection and other types of processing of personal data need to be made, the term ‘further processing’ is used.

‘Data protection’ denotes a set of legal rules that regulates the various stages involved in the processing of personal data of individuals.

‘Biometric data’, ‘biometric identifiers’, or simply ‘biometrics’, are defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow for, or confirm, the unique identification of that natural person, such as facial images or dactyloscopic data. Biometric data may be used for different purposes. Firstly, their collection and storage may be used for verification purposes (‘one-to-one’ search), under which biometric data are compared to the biometric data already registered (e.g.

---

41 Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer 2014) 37-48.
42 ibid.
44 ibid art 4(2).
45 ibid art 4(14).
under the same name). The second option, identification (‘one-to-many’ search), involves a comparison of one’s biometric data to all such data stored. This includes cases where the biometric data under comparison are used as a search tool, as these are not attributed to a known person. Despite the advantages assigned to the use of biometric data, their reliability is far from absolute. A false rejection rate (FRR) is the rate that refers to situations where a genuine user is incorrectly rejected, as opposed to a false acceptance rate (FAR) referring to situations when an intruder is incorrectly accepted.

‘Law enforcement authorities’, ‘law enforcement agencies’ or ‘law enforcement bodies’ are to be understood as the authorities responsible for the prevention, detection and investigation of criminal offences. The notion is used broadly to include both judicial and police bodies involved in crime prevention and investigation. However, intelligence agencies are not encompassed by default in these terms; where appropriate, it is explained the extent to which those bodies have access to third-country nationals’ data.

Finally, it must be noted from the outset that not all EU Member States participate in the systems under scrutiny, whereas some non-EU Member States do take part. In each Chapter, the participating States are indicated, however, for simplicity reasons, the databases are referred to as ‘EU’ systems.

5. Arrangement of chapters

This thesis comprises of six chapters, an introduction and conclusions. Chapter 1 provides the theoretical framework of this thesis. Its aim is to examine the role of privacy in the field of personal data processing under EU law. The Chapter analyses the rights to respect for private life and to the protection of personal data, calls for the centrality of the former, and puts forward a ‘check-list’ of parameters to be taken into consideration when assessing the legality of measures involving the processing of personal data. Chapters 2-4 focus on the setting up and operation of currently operational databases, namely the SIS II, the VIS and Eurodac. The sequence of chapters does not follow the chronological order in which the systems began their operation. Rather, this order is chosen bearing in mind several factors: the chronological order in which the current legal framework of each database was adopted; legislative reforms in the pipeline; and possible influence and interaction among different systems.
Chapter 5 is devoted to the proposed EES, which is due to be agreed upon in late 2016, with a view to becoming operational in 2020. Each of these chapters outlines the origins of the system in question, maps the relevant legal framework (including any reforms on the EU agenda), and analyses the privacy challenges. Finally, Chapter 6 constitutes a ‘window to the future’, by providing a concise overview of other ideas that have been under scrutiny or that will soon preoccupy the EU legislator, namely the RTP, the ETIAS, possibility of setting up a Residence Permits Repository, and interoperability among existing and forthcoming systems.
CHAPTER 1. Unravelling Ariandne’s Thread: Data Processing and Privacy in the EU Legal Order

‘Privacy has a protean capacity to be all things to all lawyers.’

1. Introduction

Much ink has been spilt in trying to clarify the legal concept of privacy, with a significant portion of the relevant scholarship being dedicated to the processing of personal data. A key characteristic in this respect is the lack of a uniform perspective in different jurisdictions. In the US, this particular aspect of privacy is referred to as ‘data privacy’ or ‘informational privacy’, and a constitutional right to data protection does not exist, which illustrates the inseparability of these concepts. By contrast, at EU level, a newborn right to personal data, enshrined in Article 8 EUCFR, coexists alongside the well-established right to privacy, as encompassed in Articles 7 EUCFR and 8 ECHR. Naturally, this coexistence raises questions regarding the relationship and bond shared between the two rights and their respective roles in assessing legal instruments involving the collection and further processing of personal data.

In this Chapter, which is meant to provide the theoretical foundations that inform the analysis of the case studies, I argue for the centrality of privacy as the appropriate framework within which instruments involving the processing of personal data should be primarily assessed, and I submit a typology of privacy standards on the basis of the relevant case law of the Strasbourg and Luxembourg Courts. In my view, the right to private life provides more effective protection to individuals than data protection law, as it questions the collection of personal data and focuses on the individual in question. This does not mean that the importance of data protection law, as exemplified by a series of data protection principles proclaimed in different international and regional

instruments, is negated. On the contrary, data protection law is viewed as being very closely connected to privacy and central in evaluating limitations to that right. Rather, what I challenge is the extent to which the right to the protection of personal data can operate on its own without recourse to privacy as a *lex specialis* to the right to privacy in the information technology field.

In this context, first I provide a concise overview of the main theories that have been elaborated over time with regard to the definition of privacy, with the modest ambition to shed light into the intricate aspects of this important, yet elusive, notion. Secondly, I focus on the legal articulation of the concept in EU primary and secondary law and put the rights to private life and personal data protection under the microscope. As the focus of the thesis is placed on the former notion, references to the latter are limited to the extent that they are necessary for the purposes of the analysis. The final sections of this Chapter are devoted to examining the judicial assessment of privacy by the ECtHR and CJEU, both in terms of how the notion of privacy is understood and in terms of the substantial protection afforded to individuals.

2. Conceptualising privacy

The question ‘what is privacy’ has preoccupied numerous legal scholars, philosophers, political scientists and sociologists only to conclude that it is extremely difficult to reach a universally satisfying definition. Wacks considers privacy as ‘large and unwieldy’ and Bennett describes it as ‘a notoriously vague, ambiguous, and controversial term that embraces a confusing knot of problems, tensions, rights and duties’. Over time, commentators have regarded privacy as ‘an unusually slippery concept’, ‘exasperatingly vague and evanescent’, ‘prone to definitional instability’,

---

48 For literature on data protection law see among others Lee Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer 2002); Christopher Kuner, *European Data Privacy Law and Online Business* (Oxford University Press 2003); González Fuster (n41).


'notorious elastic and equivocal',”54 ‘highly subjective’55 and operating ‘in a plethora of unrelated contexts’.56 Solove, more recently, has stated that privacy ‘is a concept in disarray. Nobody can articulate what it means.’57

Many different definitions have been advanced over time in order to approach the legal notion of privacy. The origins of ‘the right to privacy’ conceptualised as ‘the right to be let alone’ can be traced back to 1890, when Warren and Brandeis published their classic article.58 Reflecting on the harms caused by gossip and press intrusions into people’s private lives, they opined that ‘the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others’.59 A popular theory on privacy considers the right as a form of ‘control over personal information’. Westin conceptualised privacy as ‘the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’.60 In his view, this involved ‘when such information will be obtained and what uses will be made of it by others’.61 In Westin’s theory, information lies at the heart of the definition, and the ability of the individual to exercise some control over the use of information about them is central. Numerous authors perceive privacy as control over personal information,62 with certain commentators further linking the notion to conceiving privacy as a form of intimacy.63 However, the control-based conceptualisations of privacy have attracted considerable criticism, mainly because they do not address the voluntary disclosure of data.64 Similarly, the notion of intimacy has been considered as both too narrow and too broad; too narrow because it focuses solely on a small portion of privacy and too broad
because the scope of intimacy is not appropriately defined.\(^{65}\) Another group of scholars adhere to the ‘limited access to the self’ theory. Gavison explains the interests protected by a right to privacy in terms of delimiting a person’s accessibility to others, in particular ‘the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention’.\(^{66}\)

The last perception discussed in this section understands privacy as intertwined with personhood, self-development and individuality. In particular, Reiman regards privacy as a form of protecting ‘the individual’s interest in becoming, being, and remaining a person’,\(^{67}\) whereas Pound and Freund consider privacy as vital in order to protect a person’s integrity, but merely define it as ‘physical proximity’.\(^{68}\) This definition intersects with other rights, like the right not to be subject to violence, thus the conceptual boundaries of this interpretation of privacy are blurred. Furthermore, it is mostly used in order to explain why privacy is important, and what aspects of the self it protects.\(^{69}\)

In order to overcome the conceptual difficulties surrounding privacy, several authors have increasingly adhered to the view that rather than contemplating on the foundations of privacy, it would be more pragmatic to scrutinise privacy in its different dimensions or contexts. Solove rightly contends that the understanding of privacy is dependent upon context and that there is no common denominator to all issues understood as ‘privacy’.\(^{70}\) He asserts that privacy ‘is best used as a shorthand umbrella term for a related web of things’\(^{71}\) and puts forward a ‘taxonomy’ that concentrates on

---

\(^{65}\) Solove, *Understanding Privacy* (n57) 37.


\(^{67}\) Reiman (n71) 308.


\(^{69}\) Solove, *Understanding Privacy* (n57) 30.


the different types of activities and actions that impinge upon privacy.\textsuperscript{72} His theory revolves around four key privacy problems: 1) information collection, 2) information processing, 3) information dissemination, and 4) invasion. Another line of thinking led by Clarke conceptualises privacy through the development of a typology of four different dimensions: 1) privacy of the person, or ‘bodily privacy’, involving the integrity of someone’s body; 2) privacy of personal behaviour, which include sexual preferences and habits, political activities and religious practices; 3) privacy of personal communication, or ‘interception privacy’ involving issues such as wire tapping; and 4) privacy of personal data or ‘data privacy’ or ‘information privacy’.\textsuperscript{73} Recently, in light of recent technological advances, Finn, Wright and Friedewald updated Clarke’s theory by adding three modern types of privacy to include privacy of thoughts and feelings, of location and of association.\textsuperscript{74}

At the heart of the aforementioned approaches is the understanding of privacy as an individual right in juxtaposition with the larger community. This interplay is exemplified by the normative distinction that is made between the ‘private’ and ‘public’, the ‘private’ and the ‘public’ sphere.\textsuperscript{75} Currently, the ‘broader social importance of privacy’ is broadly recognised.\textsuperscript{76} As Regan explains, when conceiving privacy as an individual right, a necessary balancing between that and the social interest occurs. This has the effect that privacy has been on the defensive, with those invoking privacy protection having to prove that the ‘social’ interest in privacy is less important than the individual harm incurred. Similarly, Simitis considers that ‘privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone’.\textsuperscript{77} In reflecting on surveillance and the social value of privacy, Goold notes that

‘[b]y focusing on the political rather than the individual dimension of privacy, we not only free ourselves from complex discussions of individual autonomy and dignity, but also ensure that the relationship between the


\textsuperscript{73} Clarke (n23).

\textsuperscript{74} Rachel Finn, David Wright and Will Friedewald, ‘Seven Types of Privacy’ in Serge Gutwirth and others (eds), European Data Protection: Coming of Age (Springer 2013).

\textsuperscript{75} At this point, the ‘sphere theory’ (Sphärentheorie) should be mentioned. It was developed by the German Constitutional Court according to which each individual enjoyed three degrees of the private, the Individualspähre (‘social sphere’); the Privatspähre (‘a broader sphere of privacy’) and the Intimspähre (the innermost sphere). See Robert Alexy, A Theory of Constitutional Rights (Oxford University Press 2002).


individual and the state remains at the heart of any debate about privacy and surveillance.\textsuperscript{78}

The previous paragraphs serve to demonstrate that a widely agreed definition on privacy remains – and probably will remain – elusive. Nevertheless, there is a broader consensus that privacy is a multi-level notion applicable in a cluster of contexts. No single approach stemming from the theories set out above satisfactorily encapsulates the dynamics of privacy. Solove’s taxonomy presents a number of merits, not least because the different levels of identified activities largely mirror the different stages pertaining to the processing of personal data in centralised databases. Nevertheless, it may lead to fragmentary results, as it does not take fully into consideration that a single measure or instrument may impinge upon privacy in multiple ways, which severely deepen the interference. The ‘dimensional’ approach to privacy is equally a handy tool; by going-through each point in the ‘check-list’, different interferences with privacy may be highlighted. However, this approach runs the risk of potential overlaps, whereby a single activity is considered as attacking multiple dimensions of privacy. This flexibility of privacy depending upon the context within which it ‘operates’ is also apparent in the sectoral approach to privacy under EU secondary law, via the protection of personal data and the elevation of the latter as a fundamental right alongside privacy to assist particularly in the field of information technology.

3. The protection of privacy under EU law

3.1 Sources

The right to private life in the framework of personal data processing has been ‘implemented’ at EU level through the enactment of a series of legal instruments addressing various aspects of processing in different contexts. Until recently, Directive 95/46/EC,\textsuperscript{79} or, as it is commonly referred to, the Data Protection Directive, was the centrepiece of the EU privacy legal regime. It emerged out of the need to serve two

\textsuperscript{78} Jeremy Goold, ‘Surveillance and the Political Value of Privacy’ (Amsterdam Law Forum 2009).

divergent interests; to ensure the free flow of data between national regulatory systems and, thus, safeguard internal market prerogatives, whilst protecting the privacy of individuals. This dual objective of the Directive, which has been criticised as neutralising the protection of rights in favour of economic efficiency, is explicitly spelled out already from the outset. Overall, the Directive enacts a set of principles applicable for legitimate processing of personal data, envisages a series of rights afforded to individuals, and imposes obligations upon data controllers. Furthermore, transfers of data to third countries are allowed only if ‘the third country in question ensures an adequate level of protection’ and grants the Commission with the last word on the evaluation of the adequacy of protection afforded by a third country. The little sibling of the Data Protection Directive is Framework Decision 2008/977/JHA. It regulates the exchange of personal information in the context of police and judicial cooperation, thus, leaving apart domestic data processing. Although most of the provisions are meant to mirror the data protection safeguards as set out in the Data Protection Directive, their content has been heavily compromised, resulting in a significantly lower level of personal data protection than the one provided in the Directive.

82 ibid art 6. Data must be: a) processed fairly and lawfully; b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible to those purposes (purpose limitation principle); c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (data minimisation); d) accurate and up to date; and e) kept for no longer than is necessary for the purposes for which they were collected or processed.
83 ibid. These are: a right to information (art 10), right to access (art 12) and right to object (art 14).
84 ibid art 7, which enumerates six grounds that can render data processing legitimate; a) if the individual has unambiguously given their consent, or when processing is necessary: a) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; b) for compliance with a legal obligation to which the controller is subject; c) in order to protect the vital interests of the data subject; d) for the performance of a task carried out in the public interest or official authority vested in the controller; or e) for the purposes of the legitimate interests pursued by the controller.
85 ibid art 25. For exceptions see art 26.
Both instruments were recently replaced by a General Data Protection Regulation and a Data Protection Directive respectively. This broad reform was prompted by the new institutional framework post-Lisbon, particularly the insertion of Article 16 TFEU, which mandates the adoption of rules on data protection, the need to accommodate the new Internet reality, and the need to address the implementation discrepancies at the national level. Among the new features of the Regulation is that the concept of consent as a ground for legitimising data processing is clarified and individuals’ rights are strengthened. As for the new Directive, its main innovation is that it will apply to domestic processing, thus addressing its gravest shortcoming. The ‘free movement’ of data is added as one of its stated purposes, signifying that data transfers are to be permitted and streamlined through regulatory provisions. The Directive prescribes specialised rules for data processing, particularly in relation to profiling, and Member States are required to distinguish between personal data based on facts and personal data based on personal assessments, and personal data of different categories of individuals (persons against whom there are serious grounds for believing that they have committed or are about to commit a criminal offence, convicted persons, victims and other parties such as witnesses).


93 General Data Protection Regulation, arts 7, 8 and 9(2)(a). According art 4(11), consent must be ‘freely given, specific, informed and unambiguous’.

94 ibid arts 13-4, 17 and 20.


97 ibid art 7.

98 ibid art 6.
The ‘patchwork’\textsuperscript{99} of privacy regimes is complemented by numerous sector-specific pieces of legislation that complement and particularise privacy protection in different fields.\textsuperscript{100} Under this approach, which is also relevant in the context of immigration databases, each instrument constitutes \textit{lex specialis} to the Data Protection Directive or Framework Decision – depending on their material content –, thus their rules take precedence insofar as they regulate issues encompassed in the general instruments. For issues left unregulated they are complemented by the general legislative instruments (\textit{lex generalis}).

3.2 The constitutional protection of privacy and the genesis of Article 8 EUCFR

3.2.1 Introducing the ‘right to respect for private life’ (Article 7 EUCFR)

Article 7 EUCFR is a replica of Article 8 ECHR\textsuperscript{101} and stipulates that ‘[e]veryone has the right to respect for his or her private life, home and communications.’\textsuperscript{102} However, there is no paragraph equivalent to Article 8(2) ECHR defining the conditions for a justifiable limitation to the right. In view of this deliberate omission – attributed to


\textsuperscript{101} See Section 4.1.

\textsuperscript{102} Article 7 refers to a right to respect for ‘communications’, whereas Article 8 ECHR refers to ‘correspondence’. This minor amendment reflects the expansive approach of the ECHR case law, whilst taking into account the developments in communication technology. Kabera Karanja (n29) 279; González Fuster (n41) 200.
the drafters’ economy\textsuperscript{103} – Article 7 must be read jointly with the generally applicable Article 52 on the scope of guaranteed rights, which provides that:

‘Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.’

Although this provision largely reminisces of Article 8(2) ECHR, there are two differences that need to be highlighted; instead of quoting the exhaustive list of legitimate purposes stated in Article 8(2), the Charter refers to ‘objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others’, which necessarily broadens the legitimate grounds justifying limitations with the right to privacy.\textsuperscript{104} Furthermore, Article 52(1) EUCFR encompasses an additional requirement; any limitation to the right must respect the essential core of the right affected.\textsuperscript{105}

Furthermore, according to Article 52(3) EUCHR:

‘In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent the Union law providing more extensive protection.’

Given that Article 7 EUCFR unquestionably reflects Article 8 ECHR, the former needs to be understood and interpreted in light of the latter and the relevant case law elaborated by the ECtHR. In other words, the approach of the ECtHR also determines the interpretation of Article 7 EUCFR.


\textsuperscript{104} González Fuster (n41) 201. This means that when assessing a particular measure it is not necessary to directly link its stated purpose with one of the legitimate aims as stated in Article 8 ECHR.

\textsuperscript{105} The CJEU has clarified this concept in Case C-362/14 Maximilian Schrems v Data Protection Commissioner (20.10.2015). See below Section 5.2.3. Hijmans notes that this concept derives from earlier case law of the Luxembourg Court according to which the very substance of the rights should not be undermined. Hijmans (n91) 182. See Case 5/88 Wachau [1989] ECR 02609 and Case C-292/97 Karlsson and others [2000] 1-02737.
3.2.2 Introducing the ‘right to the protection of personal data’ (Article 8 EUCFR)

Next to the right to respect for private life, the Charter recognises the fundamental right to the protection of personal data. ‘[I]n unusual detail for a bill of rights’, Article 8 EUCFR establishes that:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which had been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.’

Whereas the horizontal clause of Article 52(1) EUCFR seems to be applicable, Article 52(3) EUCFR is, in principle, irrelevant, given that under the ECHR there is no corresponding right to the right of personal data protection. However, the Explanations accompanying the Charter assert that Article 8 EUCFR is based on a wide array of legal instruments and provisions; Article 8 ECHR, Article 286 EC Treaty, now substituted by Article 16 TFEU, Directive 95/46/EC and Convention No 108. Be it as it may, the recognition of data protection as a fundamental right marks a departure from both previous approaches whereby data protection served other rights and freedoms, notably privacy, but not as constituting a sui generis, specific right.

Most commentators contend that the elevation of data protection to the status of a fundamental right, and its co-existence with privacy, is a unique feature of the Charter and marks an innovation of the EU. Key in this context has been the introduction of

---

107 Council, Document 4473/00 (11.10.2000) 11. For an opposite view see Hjmans (n91) 70.
108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108.
109 Antonio Vitorino, ‘La Cour de Justice et les Droits Fondamentaux depuis la Proclamation de la Charte’ in Ninon Colneric and others (eds), Une Communauté de Droit: Festchrift für Gil Carlos Rodríguez Iglesias (Berliner Wissenschafts-Verlag 2003) 117.
Article 16 TFEU setting out a special legal basis which provides a subjective right to data protection.\textsuperscript{111} Although this is the first time that an international instrument includes such a right,\textsuperscript{112} its emergence did not occur \textit{ad nihilo}; it is true that when the first discussions on the drafting of the Charter commenced in the 1980s, data protection did not feature among the list of European fundamental rights.\textsuperscript{113} However, gradually came the realisation that the threats to \textit{privacy} arising from new technologies required the recognition of new rights.\textsuperscript{114} When, in 1999, the European Council decided the adoption of an EU Bill of Rights, the Article 29 DPWP favoured the inclusion of personal data protection, submitting that some Member States had already incorporated such a right in their own constitutions, whereas in others it had acquired constitutional status through national case law.\textsuperscript{115} In this context, the co-existence of the two rights may be seen as a recognition of, and respect for, the different constitutional approaches across Member States – those conceiving privacy as encompassing data protection, and those providing for an autonomous right to data protection.\textsuperscript{116}

Some scholars consider that the axis of data protection has shifted to give prevalence to the purpose of protecting the individual rather than to the free flow of data, thus giving ‘a more authoritative foundation’ rather than a collateral measure of the internal market.\textsuperscript{117} In other words, the elevation of the data protection to the status of a fundamental right has been seen as signaling its disentanglement from the internal market origins and emphasising its fundamental rights dimension.\textsuperscript{118} Another way of viewing the development is that the Charter granted protection to personal data


\textsuperscript{114} The Comité des Sages, established to reflect on the Charter, found that ‘new technologies are creating many problems in terms of fundamental rights: thus the information society may threaten individual privacy’. Comité des Sages, ‘For a Europe of Civic and Social rights’ (Commission 1996). See Expert Group on Fundamental Rights, ‘Affirming Fundamental Rights in the European Union: Time to Act’ (Commission 1999). Also see Brailant (n110) 47.

\textsuperscript{115} Article 29 DPWP, ‘Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights’ (WP26, 1999) 2. For an analysis on national legislations see González Fuster (n41) 66-70.


\textsuperscript{117} Hijmans (n91) 57.

\textsuperscript{118} De Hert and Gutwirth, ‘Data Protection in the Case Law of Strasbourg and Luxembourg’ (n116) 8-9.
independently of privacy and outside of its scope, hence flagging the difference between the two concepts. In this context, the development has been regarded as a golden opportunity for individuals to rely directly on this right for alleged violation of the protection of personal data without the need to have recourse to the right to private life.\textsuperscript{119}

3.3 Privacy and data protection – ‘Dangerous liaisons’?

The recognition of data protection as a fundamental right alongside privacy has acted as a major stimulus for revisiting the role of the two concepts and the exact nature of their relationship. Before 2000, it was fairly established that the right to respect for private life incorporated the protection of personal data as one of its components; the former being understood as a broader notion than the latter. In this framework, the protection of personal data was often regarded as the ‘informational dimension’ of the right to privacy.\textsuperscript{120}

However, since the EU constitutional entrenchment of a right to data protection, scholars have engaged into a lively debate as to whether data protection should be depicted as an ‘autonomous’\textsuperscript{121} or a ‘separate’\textsuperscript{122} fundamental right, ‘distinct’\textsuperscript{123} from the right to privacy, or whether it merely remains a component of privacy. Reactions from data protection scholars vary in this respect. Rodotá states that the emergence of Article 8 EUCFR ‘can be considered the final point of a long evolution, separating privacy from data protection’.\textsuperscript{124} González Fuster more cautiously notes that the disentanglement of the rights is still an ongoing process, but by acquiring the legal status of a fundamental right, data protection has made a key step towards that

\textsuperscript{119} Kabera Karanja (n29) 87.
\textsuperscript{120} Karim Benyekhlef, ‘Les Normes Internationales de Protection des Données Personnelles et l’ Autoroute de l’ Information’ in Les Journées Maximilien-Caron, Le Respect de la Vie Privée dans l’Entreprise (Thémis 1996) 91. This approach should be seen as directly influenced by the dynamic approach of the ECtHR. See Section 4.
\textsuperscript{121} Stefano Rodotá, ‘Data Protection as a Fundamental Right’ in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer 2009) 79.
\textsuperscript{122} Hustinx (n92) 16.
\textsuperscript{124} Rodotá (n121) 79; Kranenborg contends that the inclusion of separate provisions signifies a distinction between the two notions, without specifying the relationship between the two rights and the nature of this distinction. Herke Kranenborg, ‘Article 8 - Protection of Personal Data’ in Steve Peers and others (eds), The EU Charter of Fundamental Rights - A Commentary (Hart 2014).
De Hert and Gutwirth enthusiastically state that ‘something is happening at constitutional level.’

To reconcile the co-existence of the two concepts, whilst taking note of the original anchoring of data protection to privacy, a number of commentators recognise that privacy and data protection are ‘closely related’, or in more neutral terms ‘interact in a variety of ways’. This peculiar relationship has been codified as a partial overlap, enabling a synthesis of the two approaches; the traditional line of thinking, whereby data protection constitutes an integral facet of private life, and the modern one in which data protection is a different notion. The partial overlap approach seems to foster the idea that data protection is integral to privacy whilst remaining autonomous at the same time. I agree with the proposition that privacy and data protection are not identical notions. By default, privacy is wider than data protection in that it encompasses a multiplicity of aspects apart from the processing of personal data, whereas data protection seems to largely fall within this aspect of privacy that is known as the ‘control over personal information’ theories. Furthermore, even the most dedicated advocates of data protection admit that the latter is a tool for safeguarding privacy – at least to some extent – but that does not operate the other way around. In practice, given the wide and flexible interpretation of the right to private life, the overlap between the two concepts is quite heavy, to the extent that privacy subsumes data protection to a great extent. However, I argue that autonomous recourse to data protection does not offer the same level of protection as privacy, because, apart from the quantitative difference between the two notions, there is also a qualitative ‘superiority’ of privacy stemming from the ambiguities and limitations in the nature and role of data protection.

125 González Fuster (n41) 260-1.
126 De Hert and Gutwirth, ‘Data Protection in the Case Law of Strasbourg and Luxembourg’ (n116) 7.
129 González Fuster (n41) 214-5.
130 Rodotà (n121) 79.
3.4 The ‘anatomy’ of the right to the protection of personal data – Conceptual ambiguities leading to inherent limitations

3.4.1 Ambiguities stemming from the wording of Article 8 EUCFR

A close look into the wording of Article 8 EUCFR reveals a conceptual controversy regarding its core content. Two hypotheses have been advanced in this respect, broadly summarised as the ‘prohibitive’\textsuperscript{133} and the ‘permissive’\textsuperscript{134} approaches.\textsuperscript{135}

\begin{itemize}
\item[a)] The ‘prohibitive’ approach
\end{itemize}

In the first hypothesis, the right to personal data protection and the right to private life share a conceptual link based on the notion of informational self-determination, as developed by the German Constitutional Court in its landmark Census decision of 1983.\textsuperscript{136} In that judgment the Court opined that the individual must be empowered to determine for themselves the disclosure and use of their personal data.\textsuperscript{137} Understanding data protection as flowing from the notion of informational self-determination, Article 8 EUCFR prescribes an overall prohibition of the processing of personal data, involving all aspects of processing including the collection, thus signifying that individuals are entitled to have their personal data shielded.\textsuperscript{138} Data protection is essentially aimed at

\textsuperscript{133} For proponents of this approach see Birte Siemen, Datenschutz als Europäisches (Duncker & Humblot 2006) 283; Orla Lynskey, ‘Deconstructing Data Protection: The “Added-Value” of a Right to Data Protection in the EU Legal Order’ (2014) 63(3) International Comparative Law Quarterly 569. Tzanou calls for a prohibitive approach to data protection albeit recognising that the wording of Article 8 ECFR suggests that data protection is permissive in nature. Tzanou (n31) 52-4.


\textsuperscript{135} These approaches are codified by González Fuster and Gutwirth (n134).

\textsuperscript{136} Decision BVerfGE 65 1 of the German Constitutional Court (15.12.1983).


\textsuperscript{138} This right is comparable to ownership of personal data. See Nadezhda Purtova, ‘Property Rights In Personal Data: Learning from the American Discourse’ (2009) 25(6) Computer Law & Security Review 507.
reducing information and power asymmetries in an information society,\textsuperscript{139} by granting to the individual the control over whether and how their data would be processed. In this framework, the right should be considered as an exception to the general rule according to which the first Articles of the Charter define the protected rights, whereas the final general provisions are applicable to all the prescribed rights.\textsuperscript{140} Consequently, mirroring the text of Article 8 ECHR, the content of the right to the protection of personal data is concentrated on Article 8(1) and the second and third paragraphs enumerate the conditions for its lawful limitation, stating when and how personal data may be processed.\textsuperscript{141} An argument in support of this approach would be that Article 8(1) EUCFR is worded in affirmative and unconditional terms. Furthermore, one could also claim that the presumption of prohibition is embedded in Article 8 of the Data Protection Directive prohibiting the processing of sensitive personal data.\textsuperscript{142} Nevertheless, counter-arguments in this respect would be the fact that Article 8(2) of the Data Protection Directive is fraught with exceptions and that nowhere in Article 8 EUCFR is such prohibition expressly mentioned.\textsuperscript{143}

**b) The ‘permissive’ approach**

In turn, under the permissive approach, a right to prevent processing of personal data \textit{per se} does not exist in EU law. Article 8 EUCFR is conceptualised as following the structure of the Charter and, thus, should be read as a unitary provision. From this perspective, taken as a whole, the nucleus of the right is precisely described by the conditions allowing for the processing of personal data, which are the six requirements set out in paragraphs (2) and (3). So long as these requirements are fulfilled, processing of personal data is assumed, in principle, to be allowed. In other words, ‘the requirements of Article 8(2) and 8(3) would not outline demands applicable to interferences with the right, but those of the very right itself, which is thus expressed and substantiated through them.’\textsuperscript{144} Hustinx, the former EDPS, endorses the permissive approach noting that:

‘[Article 8 EUCFR] was not designed to \textit{prevent} the processing of such information or to \textit{limit} the use of information technology \textit{per se}. Instead, it

\textsuperscript{139} Lynskey (n133) 592ff.
\textsuperscript{140} Siemen (n133) 283.
\textsuperscript{141} ibid.
\textsuperscript{142} Hijmans (n91) 61.
\textsuperscript{143} ibid.
\textsuperscript{144} González Fuster and Gutwirth (n134) 533.
was designed to provide safeguards whenever information technology would be used for processing relating to individuals.\textsuperscript{145}

In this context, an interference with the right cannot arise from the mere fact that personal data has been processed; as Docksey points out, the processing of personal data is a condition for the application of Article 8 EUCFR, not an interference with it.\textsuperscript{146}

Interference can only stem from the fact the data protection principles outlined in Article 8(2) and 8(3) have not been respected.\textsuperscript{147}

This hypothesis broadly corresponds to a popular theory put forward by De Hert and Gutwirth delineating the roles of privacy and data protection in a democratic constitutional State.\textsuperscript{148} Their theory is grounded on the premise that privacy and data protection can be regarded as two distinct tools of power control that perform separate, yet complementary, functions. In an attempt to define their differences in scope, rationale and logic, they categorise the two notions in terms of opacity v transparency tools. Privacy is understood as forming part of the opacity tools, which ‘embody normative choices about the limits of power’, whereas data protection is conceived as a transparency tool that becomes relevant ‘after these normative choices have been made in order still to channel the normatively accepted exercise of power.’\textsuperscript{149} In this framework, while the key feature of privacy lies in the fact that it serves to protect individuals by saturating their opacity before power, by drawing normative lines against illegitimate and excessive use of power, data protection aims at enhancing the transparency of power’s exercise by organising and regulating the ways in which any data processing must be carried out in order to fulfil the lawfulness requirement.\textsuperscript{150} As Gutwirth has noted elsewhere,

‘[w]hilst privacy builds a shield around the individual, creating a zone of autonomy and liberty, data protection puts the activity of the processor in the spotlight, gives the individual subjective rights to control the processing of his/her personal data and enforces the processor’s accountability.’\textsuperscript{151}

Pursuant to this approach, privacy constitutes a prohibitive rule, questioning at a first stage whether the collection and further processing of personal data should in principle

\textsuperscript{145} Hustinx (n92) 1. Emphasis original.
\textsuperscript{146} Docksey (n134) 3.
\textsuperscript{147} Hustinx (n92) 18. Hujmans agrees as regards this point, but argues that Article 52(1) is not relevant to data protection. Hujmans (n91) 64 and 66.
\textsuperscript{149} ibid 70.
\textsuperscript{150} ibid 61-65.
\textsuperscript{151} Serge Gutwirth and others, ‘Preface’ in Reinventing Data Protection? (Springer 2009).
take place, whereas data protection serves as a permissive rule of ‘pragmatic’ nature, as it is based on the assumption that personal data processing is, in principle, allowed, therefore, its role is reserved to setting out ‘the rules of the game’.

The permissive approach gains ground for a number of reasons; first, placing the individual in control of their data necessarily entails that consent of the individual is necessary at all times, which is not in line with Article 8(2) EUCFR, according to which processing is legitimate also if prescribed in law. Second, the permissive approach fits well with the dual rationale behind the configuration of data protection safeguards, whereby the free flow of data must be ensured to the extent possible. The establishment of a novel right to personal data protection would seem an unrealistic development, particularly in light of ‘big data’. A third argument in favour of the permissive notion stems from the drafting history of the Charter. The Convention that prepared the text had, in fact, considered the inclusion of a right to information self-determination in Article 8 EUCFR close to the prohibitive approach to data protection, but this idea was rejected, leading to the current version of the Article. The fact that its wording underwent this fundamental change is a strong indication that the second hypothesis must prevail. Besides, when its current wording was finally decided upon, the draft Article appeared as a single paragraph, thus as a unified provision.

3.4.2 ‘Deconstructing’ the right to the protection of personal data – Privacy as providing more holistic protection

The prevalence of the second hypothesis with regard to the nature of the right to the protection of personal data reveals the ‘Achilles heel’ of EU data protection law. The wording of Article 8 EUCFR confirms the main point advanced by De Hert and Gutwirth regarding the division of tasks between privacy and data protection. Whilst

---

152 De Hert and Gutwirth ‘Privacy, Data Protection and Law Enforcement’ (n148) 77.
153 Hijmans (n91) 63-66.
154 Gellert and Gutwirth note that according to Article 1(1) of the Data Protection Directive, the aim of the data protection is to ‘regulate a specific practice’. Gellert and Gutwirth (n131) 525.
155 Hijmans (n91) 62.
156 In an early formulation of the EUCFR, the right to data protection is envisaged as follows: ‘Everyone has the right to determine for himself whether his personal data may be disclosed and how they may be used’ The article goes on stating that ‘[i]n any case, data protection is an aspect of respect for privacy’. See Council, Document 4284/00 (05.05.2000) 19. In another draft, the right is depicted in this manner: ‘Everyone shall have the right to determine for himself the disclosure and use of his personal data and to obtain information on their storage provided that this right does not conflict with the rights of third persons, and ‘restrictions shall be admissible by law only in the dominant general interest’. See Council, Document 4102/00 (06.01.2000) 6.
their theory could be criticised in that it strives for a clear-cut separation between the two concepts, thus disregarding their close bond and the inherent limitations of EU data protection law, it correctly identifies that processing of personal data in general is ‘almost a natural presumption’ and an activity endorsed by the EU legislator, as long as a series of principles are respected. As Gellert and Gutwirth observe, ‘data protection by default accepts the processing of personal data; otherwise its aim would be void’. In this respect, the role of data protection is not to create zones of non-interference by the State, but by assuming that personal data can be processed, provides a system for ‘checks and balances’. The very rationale of data protection is procedural, rather than substantial and its role is limited to following and regulating in detail different instances of personal data processing through the development of key legal principles or rules on remedies for the individual. Consequently, it will come into play only at a later stage, in order to minimise the impact of the processing. As such, it cannot challenge whether the collection of personal data, which is the first stage in information processing, will in principle take place, but it will merely assist in identifying the modalities of such collection or of further stages of processing. Whilst it is true that the structural formulation renders data protection more ‘tangible’ than privacy, which is difficult to capture in precise terms, data protection cannot guarantee a certain level of opacity as privacy does. In fact, it may actually hinder the substantial engagement with privacy claims by de-politicising and de-valuing them into data protection safeguards. This is particularly relevant to State surveillance activities. Reliance on the right to data protection on its own does not suffice to determine the limits of the use of surveillance practices, and questions regarding the political choice to establish measures involving the collection and further processing of personal data may transform into a mere procedural checklist. These dangers may in fact lead to significantly lower the level of protection afforded to individuals, and thus runs counter to the telos of the Charter, which is to strengthen the protection of fundamental rights in

158 De Hert and Hutwirth, ‘Privacy, Data Protection and Law Enforcement’ (n148) 77.
160 Gellert and Gutwirth (n131) 525. Emphasis original.
163 Bellanova (n162) 114.
‘light of changes in society, social progress and scientific and technological developments’.\textsuperscript{164}

There are a few more limitations attached to data protection law that render the right to private life the appropriate framework for providing more holistic protection to individuals. Whereas data protection is focused on the various categories of personal data,\textsuperscript{165} privacy is centred on the individual ‘in terms of identity and the Self’, therefore, it is ideally placed to assess the impact of measures to individuals and their established relationship with the State.\textsuperscript{166} As Mitsilegas has noted, the inherent flexibility of privacy as a notion and a right allows it to evolve over time and adapt to technological developments, where the specificity of data protection may result in fragmented solutions and ultimately ‘miss the big picture’.\textsuperscript{167} Key in this context is the existence of the fragmentary EU data protection framework, whereby different activities are subject to different rules. This limitation is further linked to another characteristic of data protection; that it ‘appears easy to re-orient, if not to bend, so that many security measures, provide for their own ad hoc data protection regime’.\textsuperscript{168}

In view of the above, although the aim behind the elevation of data protection to the status of a fundamental right may have been noble, the extent to which it can offer effective protection as a self-standing right is highly doubtful. Caught in-between divergent rationales and essentially delimited in its mandate, the right to data protection remains inextricably linked to the right to private life and cannot be considered as a \textit{lex specialis} in the field of information technology\textsuperscript{169} operational on its own and interchangeable with privacy in this context. Neither can it be considered as privacy in the particular field of information processing.\textsuperscript{170} This could only have been the case if the prohibitive theory of data protection substantiated, but this approach contradicts the logic of EU data protection law as developed to balance between internal market prerogatives and protection of individuals. What could be argued is that the right to the protection of personal data forms part of privacy to a very large extent, it is one of its elements and bears considerable importance to the extent that it needs to be

\begin{footnotesize}
\begin{enumerate}
\item[164] Preamble to EUCFR.
\item[165] Bennet and Raab contend that ‘[d]ata protection concentrates disproportionately on the data rather than the person as the object of protection’. Bennet and Raab (n55) 11.
\item[166] Mitsilegas, ‘The Value of Privacy’ (n134) 107.
\item[167] Ibid 106.
\item[168] Bellanova (n162) 114.
\end{enumerate}
\end{footnotesize}
acknowledged properly, particularly in a digital era. Viewed this way, there appears to be a hierarchical and ‘chronological’ relationship between the two rights, whereby as a first step, privacy may question the normative choice of a measure, whilst as a second step, data protection will reinforce protection by providing the ‘rules of the game’. It is crucial in this respect to continue considering that the protection of personal data has its roots in the values underpinning privacy. As Rouvroy and Poullet eloquently state:

‘[b]y placing the right to data protection on the same level as privacy, the European text carries the risk that the fundamental anchoring of data protection regimes in the fundamental values of dignity and autonomy will soon be forgotten by lawyers and that legislators will soon forget to refer to these fundamental values in order to continuously assess data protection legislation taking into account the evolution of Information Society.’

These considerations regarding the potential of Articles 7 and 8 EUCFR stem merely from a theoretical analysis of the provisions. However, the centrality of privacy in assessing legal instruments involving the processing of data is further attested by the jurisprudence of both the Strasbourg and Luxembourg Courts. The following sections aim at shedding light in this regard.

4. Judicial assessment of privacy: The jurisprudence of the ECtHR as a source for inspiration

4.1 Introducing ‘the right to respect for private life’ (Article 8 ECHR)

Emerged in international law in the aftermath of the Second World War, the right to private life is envisaged in all major international and regional instruments of human rights, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the American Convention on Human Rights. In Europe, the right is listed among the human rights and fundamental freedoms of the ECHR concluded in 1950 within the framework of the Council of Europe.

\(^{171}\) Meyer (n169) art 8 ¶6; Boehm (n32) 124-5.

\(^{172}\) Rouvroy and Poullet (n128) 71.

\(^{173}\) UDHR, art 12.

\(^{174}\) ICCPR, art 17.

\(^{175}\) American Convention on Human Rights, art 11.
Article 8 of the Convention, which is applicable to everyone within the jurisdiction of the contracting parties, stipulates that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

The ECtHR has a long track record in safeguarding the protection of the four-fold right to privacy – private life, family life, home and correspondence- as set out in the Convention. Overall, Article 8 ECHR, as seen by the Strasbourg Court, entails two types of obligations: a negative and a positive one. The negative obligation signifies that states ought to abstain from taking certain actions, therefore, to ensure an exercise of the right free of interference unless the conditions of Article 8(2) are fulfilled. In this regard, the Court takes a two-step approach, which can be referred to as the ‘interference-justification’ approach; at a first stage, the aim is to substantiate whether there is an interference with the right. If so, at a second stage, it examines whether the interference is allowed by existing national law; whether there exists a legitimate aim, in particular one of those exhaustively indicated, and whether the measure in question is necessary, a condition which in practice embeds a proportionality test. The positive obligation requires states to adopt measures and provide resources designed to ensure protection of individuals from interference with their privacy by others.

---

176 ECHR, art 1.
4.2 The ECtHR on the definition of privacy: Endorsing constructive flexibility

In Section 2, I mentioned that defining privacy has been a laborious task. Numerous elements outlined there have made their way into the Strasbourg Court’s reasoning, but overall, the latter has granted to the wording of Article 8 ECHR a wide and generous interpretation. In *Niemietz v Germany*, it chose not to give a clear definition of this right by stating that it ‘does not consider it possible or necessary to attempt an exhaustive definition of the notion of “private life”’. It pointed out that ‘it would be too restrictive to limit the notion to an “inner circle” in which the individual may live his own private life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle’. It further ascertained that protection is not to be limited to the private sphere or the home of the individual as ‘[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings’. In this context, it did not exclude activities of a professional or business nature ‘since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest opportunity of developing relationships with the outside world’.

In subsequent cases, the ECtHR has consistently highlighted the wideness of the concept of private life by portraying it as ‘a broad term not susceptible to exhaustive definition’. Privacy is understood more than merely a right to intimacy, as Article 8 ECHR may protect the public conduct of individuals. In *PG and JH v UK*, the Court contended that ‘there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life”’. Furthermore, it acknowledged the existence of a right to make essential personal choices and that individual autonomy (or self-determination) is an important principle underpinning its approach and interpretation of the right to privacy. In *Pretty v UK*, the Court held for the right to private life:

182 ibid.
183 ibid.
184 ibid.
186 Gellert and Gutwirth (n131) 524.
187 *PG and JH v UK* (n185) ¶56, as reiterated in *Peck v UK* (n185) ¶57 and *Von Hannover v Germany* (2005) 40 EHRR 1 ¶50.
188 Gellert and Gutwirth (n131) 524.
‘It covers the physical and psychological integrity of a person […] It can sometimes embrace aspects of an individual’s physical and social identity […] Though no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees’. 189

In other judgments, the Court has embraced other concepts linked to privacy. For example, in *Evans v UK*, the Court intertwined private life with the individual’s physical and social identity and right to personal development,190 whereas in *Odièvre v France* it added that ‘[t]he preservation of mental stability is […] an indispensable precondition to effective enjoyment of the right to respect for private life’.191 The societal value of privacy has also been recognised; in *von Hannover v Germany*, the Court stressed that a fair balance has to be struck between competing interests of the individual and the community in regard to privacy.192 Freedom of movement has also been considered as ‘essential for the development of private life’ especially in cases where people have family, occupational or economic ties in more than one country.193

Recently, the Court summarised its findings in *S and Marper v UK* holding that:

‘Elements such as gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 […] Beyond a person’s name, his or her private and family life may include other means of personal identification and of linking to a family. […] Information about the person’s health is an important element of private life. […] The Court furthermore considers that an individual’s ethnic identity must be regarded as another such element. […]’.194

According to the Strasbourg Court, privacy is not self-explanatory and is very much fact-sensitive.195 The Court does not endorse a specific, clear-cut, one-size-fits-all definition of privacy, but rather proceeds on a case-by-case basis by attaching to the concepts autonomous meanings depending on the specific context. Therefore, it favours a holistic approach by acknowledging that privacy incorporates more aspects than the mere need to be left alone.196 Furthermore, it has been pointed out that by incorporating

---

189 Pretty v UK (n185) ¶61.
190 Evans v UK (2008) 46 EHRR 34 ¶71.
192 Von Hannover v Germany (n187) ¶57.
193 İletmiş v Turkey (2011) 52 EHRR 35 ¶50.
196 Nicholas Hatzis, ‘Giving Privacy is Due: Private Activities of Public Figures in von Hannover v Germany’ (2005) 16(1) *The King’s College Law Journal* 143.
different concepts of privacy within its case law, it seems to promote a ‘liberty’ rather than a ‘bundle of subjective rights’ approach to privacy. This approach has inevitably attracted criticism with some commentators considering the right as ‘ill-defined and amorphous’ and ‘scolding’ the Court for its ‘unwillingness’ or avoidance to identify categories permitting a clear classification of the content of the right. Whilst an author argues that a lack of a precise definition may raise legal certainty concerns, I consider that this approach allows for constructive flexibility, which is a necessary component and, therefore, an added value of privacy. Flexibility enables adaptation to social, legal and technological developments. Such adaptation is important and – even necessary – for assimilating the dynamic nature of intrusive technologies and mechanisms, particularly those related to the processing of personal data. Furthermore, as Bygrave points out, flexibility of privacy compensates for its rhetorical counterclaims, such as freedom of inquiry, the right to know, freedom of expression and liberty of the press. Besides, this understanding is in line with the evolutionary and dynamic character of the Convention. In light of this constructive flexibility the ECtHR has been able to interpret the ECHR in a dynamic and progressive manner. As a result, private life has been depicted as a multi-faceted notion encompassing inter alia gender, a person’s reputation and the processing of personal data, which is discussed in detail below.

4.3 The processing of personal data as an aspect of private life

In view of the rapid technological evolution, it was a matter of time before the Court was faced with cases relating to various aspects of personal data processing. The flexible notion of privacy allowed the Court, already since the 1980s, to hold that

---

197 François Rigaux (ed),  *La Vie Privée, Une Liberté Parmis les Autres?* (Larcier 1992); Serge Gutwirth, *Privacy and the Information Age* (Rowman & Littlefie 2002). By contrast, Whitman considers that the US approach to privacy is closer to the liberty notion, whilst the EU model is closer to dignity. Whitman, ‘The Two Western Cultures of Privacy’ (n51).
200 Bygrave, ‘The Place of Privacy in Data Protection Law’ (n132) 278.
201 The ECtHR has repeatedly emphasised that the ECHR is a ‘living instrument’ and as such its interpretation enables immediate adjustment to specific situations. See for example *Tyrer v UK* (1979-80) 2 EHRR 1 ¶31; *Loizidou v Turkey* (1997) 23 EHRR 513 ¶71; *Mamatkulov and Askarov v Turkey* (2005) 41 EHRR 25 ¶121.
202 *Van Kück v Germany* (n179); *B v France* (1993) 16 EHRR 1.
personal data protection is an issue falling within the scope of the right to private life, even though this issue was not explicitly included within the context of Article 8 ECHR. The relationship between the two concepts was highlighted in *MS v Sweden* where it was held that ‘the protection of personal data […] is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention’.\(^{204}\) In this context, the Court understands the protection of personal data as instrumental for the effective protection of privacy.

The Court’s approach should be read in conjunction with other developments within the Council of Europe, particularly the signature of Convention No 108 for the Protection of Individuals with regards to Automatic Processing of Personal Data.\(^{205}\) The Convention not only put forward the legal notion of data protection (deriving from the German *Datenschutz*), but also noted that this concept served privacy, which was already equated with Article 8 ECHR. Overall, the Convention provides the blueprint for harmonisation of data protection legislations at the national level by prescribing a set of data protection principles, with particular emphasis on data quality,\(^{206}\) special categories of data,\(^{207}\) data security\(^{208}\) and procedural rights.\(^{209}\)

In this framework, in a series of cases, the Strasbourg Court has addressed privacy concerns in relation to telephone conversations,\(^{210}\) telephone numbers,\(^{211}\) computers,\(^{212}\) video surveillance,\(^{213}\) voice recording,\(^{214}\) and the Internet.\(^{215}\) The Court has made a distinction between cases involving the processing of personal data that implicate privacy and cases that do not. At a first stage, the Court examines the extent to which the information is of a personal nature, as mandated by the Convention.\(^{216}\) If the data are intrinsically linked to the privacy of the person, the processing will fall under Article 8 ECHR without further consideration.\(^{217}\) Nevertheless, if the data are not fundamentally private, the Court examines the type and extent of processing. This involves an analysis of whether data have been stored systematically, or whether there is a focus on the data

---

\(^{204}\) *MS v Sweden* (1999) 28 EHRR 313 ¶41, as reiterated in *S and Marper v UK* (n194) ¶103.

\(^{205}\) See n108.

\(^{206}\) ibid art 5.

\(^{207}\) ibid art 6.

\(^{208}\) ibid art 7.

\(^{209}\) ibid art 8.


\(^{211}\) Malone v UK (1985) 7 EHRR 14; *PG and JH v UK* (n185); *Copland v UK* (2007) 45 EHRR 37.

\(^{212}\) Leander v Sweden (1987) 9 EHRR 433; *Amann v Switzerland* (n210); *Rotaru v Romania* (2000) 8 BHRC 43.

\(^{213}\) Peck v UK (n185); Perry v UK (2004) 39 EHHR 3.

\(^{214}\) *PG and JH v UK* (n185).

\(^{215}\) *Copland v UK* (n211).

\(^{216}\) Gellert and Gutwirth (n131) 526.

\(^{217}\) *Smith v UK*, Appl no 39658/05 (admissibility decision of 04.01.2007).
subject even if the storage is not in a systematic manner, or whether the data subject could reasonably expect the processing.\(^\text{218}\) In \textit{Khelili v Switzerland},\(^\text{219}\) it codified its approach by proclaiming that important factors to be taken into consideration are the context in which the data had been collected and stored, their nature, the way they were used and treated and the results obtainable from the processing.\(^\text{220}\)

As for the protection afforded, in \textit{Rotaru v Romania}, the Strasbourg Court clarified that Article 8 ECHR is interpreted so as to endorse the data protection guarantees envisaged in Convention No 108.\(^\text{221}\) Over the course of time, it has recognised a number of principles, albeit in an ‘incidental, rather than intended’\(^\text{222}\) manner – which can be attributed to its approach to assess privacy on a case-by-case basis; a right to access personal files,\(^\text{223}\) a right to correct it has accepted applications to correct official sexual data,\(^\text{224}\) and a right to deletion of personal data included in public dossiers.\(^\text{225}\) Importantly, the Court has recognised the purpose limitation principle, when personal data cannot be used beyond what is normally foreseeable.\(^\text{226}\) The need to establish independent supervisory authorities\(^\text{227}\) and the right to seek financial redress have also been recognised.\(^\text{228}\) Overall, viewing data protection through the privacy prism signifies that the outer remits of data protection coincide with the realms of the scope of the right to private life, thus leading Siemen to argue that the scope of data protection reaches so far as the scope of the right to respect for private life.\(^\text{229}\)

\section*{4.4 Determination of interference under Article 8(1) ECHR}

The case-by-case approach of the Strasbourg Court means that the notion of the interference is open-ended.\(^\text{230}\) In different judgments, the Court has concluded that there had been an interference with privacy due to different governmental activities involving

\begin{footnotesize}
\begin{enumerate}
\item Friedl \textit{v Austria} (1996) 21 EHRR 83; Gellert and Gutwirth (n131) 526.
\item Khelili \textit{v Switzerland}, Appl no 16188/07 (18.10.2011).
\item ibid ¶55.
\item Rotaru \textit{v Romania} (n212) ¶43.
\item Kabera Karanja (n29) 89.
\item Gaskin \textit{v UK} (n179); McMichael \textit{v UK} (1995) 20 EHRR 205; Guerra and Others \textit{v Italy} (1998) 26 EHRR 357; McGinley \textit{v UK} (1999) 27 EHRR 1.
\item Leander \textit{v Sweden} (n212); Segerstedt-Wiberg \textit{v Sweden} (2007) 44 EHRR.2.
\item Peck \textit{v UK} (n185) ¶62; Perry \textit{v UK} (n213) ¶40; PG and JH \textit{v UK} (n185) ¶59; Lupker and Others \textit{v the Netherlands} Appl no 18395/91 (Commission Decision, 07.12.1992); Friedl \textit{v Austria} (n218).
\item Klass \textit{v Germany} (n210) ¶55; Leander \textit{v Sweden} (n212) ¶63-67; Rotaru \textit{v Romania} (n212) ¶59-60. See Gaskin \textit{v the UK} (n179); Z \textit{v Finland} (1998) 25 EHRR 371.
\item Rotaru \textit{v Romania} (n212) ¶83. See Gaskin \textit{v UK} (n179) ¶55-58.
\item Siemen (n133) 57.
\item Boehm (n32) 33.
\end{enumerate}
\end{footnotesize}
the processing of personal data such as secret surveillance and recording;\textsuperscript{231} wire
tapping;\textsuperscript{232} interception via GPS;\textsuperscript{233} the recording of a person’s voice;\textsuperscript{234} the unwanted
watching and recording in private or even public places;\textsuperscript{235} the dissemination of photos
or videos.\textsuperscript{236} It has also dealt with sensitive data such as DNA samples and
fingerprints\textsuperscript{237} and health data.\textsuperscript{238}

For the purposes of this thesis, cases involving the systematic collection and
storage of personal data merit special attention. Perhaps the cornerstone of the
Strasbourg’s case law on the storing and further processing of public information about
individuals is the \textit{Leander v Sweden} case.\textsuperscript{239} The applicant was temporarily hired as a
museum technician at the naval museum on a Swedish military base. Based on
information stored in a secret register held by the Swedish secret services, he was asked
to leave his work without being informed of the reasons of this decision. As early as
1987, the Court found it uncontested that the register contained information related to
the applicant’s private life.\textsuperscript{240} Furthermore, it highlighted that both the storing and the
release of the information contained in the register, coupled with the refusal to allow Mr
Leander to refute it amounted to an interference with his right to private life.

This approach was confirmed in subsequent cases. \textit{Amann v Switzerland}\textsuperscript{241}
involved the drawing up of a card for the national security index on the basis of the
interception of a call. Drawing on its conclusions in \textit{Niemietz} regarding the inclusion of
activities of a professional or business nature within the notion of private life, the
Strasbourg Court found an interference with Article 8(1).\textsuperscript{242} Arguments that the card
index did not contain sensitive data and had possibly never been consulted, or that the
applicant was not inconvenienced in any way were dismissed by the Court.\textsuperscript{243} In its
view, it sufficed that data relating to the private life of a person was stored by a public
agency in order to conclude that ‘the creation and storage of the impugned card’
amounted to an interference.\textsuperscript{244}

The issue of systematically collecting and storing personal information was further

\begin{itemize}
\item \textsuperscript{231} \textit{Klass v Germany} (n210); \textit{Liberty v UK} (2009) 48 EHRR 1.
\item \textsuperscript{232} \textit{Kopp v Switzerland} (1999) 27 EHRR 91; \textit{Khan v UK} (2012) 55 EHRR 30.
\item \textsuperscript{233} \textit{Uzun v Germany} (2011) 53 EHRR 24.
\item \textsuperscript{234} \textit{PG & JH v UK} (n185).
\item \textsuperscript{235} \textit{Perry v UK} (n213).
\item \textsuperscript{236} \textit{Peck v UK} (n185).
\item \textsuperscript{237} \textit{S and Marper v UK} (n194).
\item \textsuperscript{238} \textit{Z v Finland} (n227).
\item \textsuperscript{239} \textit{Leander v Sweden} (n212).
\item \textsuperscript{240} ibid ¶48.
\item \textsuperscript{241} \textit{Amann v Switzerland} (n210).
\item \textsuperscript{242} ibid ¶65.
\item \textsuperscript{243} ibid ¶68.
\item \textsuperscript{244} ibid ¶70.
\end{itemize}
elaborated in *Rotaru v Romania*, where the defendant tried to argue that Article 8 ECHR was not applicable to the case because the information stored related to the applicant’s public life rather than his private life. The facts of this case involved a lawyer who had initiated proceedings against the Romanian Intelligence Service in relation to files including information about his alleged membership of a legionnaire movement and on publication of two anti-government pamphlets. The Court held that public information may fall within the realms of private life concretely when ‘systematically collected and stored in files held by the authorities and this is all the truer when such information concerns a person’s distant past’. In this context, it found that ‘both the storing of the information and the use of it [...] amounted to interference’. As pointed out, by this statement the Court made clear that categorising information as relating to private life shall not be read as opposed to public information. The Court’s ruling is another indication of its tendency to understand privacy widely. Although the information stored by the Romanian agency was public and, according to the Government, the applicant had waived his right to anonymity by engaging in political activities, the Court made clear that storing information about a person’s life fell within the scope of Article 8.

Another key judgment is *S and Marper v UK*, where the ECtHR dealt with two non-convicted individuals who wanted their personal information obtained by the police, including their fingerprints, DNA profiles and cellular samples, removed from the UK criminal identification database in which these were held indefinitely. The Court distinguished between different types of biometric data, cellular samples and DNA profiles on the one hand, and fingerprints on the other. While it acknowledged that cellular samples are of a highly personal nature and contain much sensitive information about an individual, with regard to fingerprints it contended that they do not contain as much information as cellular samples and DNA samples, but still ‘they contain certain external identification features much in the same way as, for example,

---

245 *Rotaru v Romania* (n212).
246 ibid ¶42.
247 ibid ¶43.
248 González Fuster (n41) 99.
250 *S and Marper v UK* (n194) ¶73.
251 ibid ¶78.
photographs or personal samples’. It clarified that:

‘fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant’.

In view of this, the Court held that the retention of fingerprints on the authorities' records are to be regarded as constituting an interference with the right to respect for private life ‘notwithstanding their objective and irrefutable character’. Importantly, it highlighted that the retention of fingerprints was not ‘inconsequential, irrelevant or neutral’.

Another issue for further exploration is the extent to which the storage of photographs triggers the application of Article 8. The decisive factors in this respect are whether the photographs were taken in relation to public or private matters and the consent of the person whose photograph has been taken. Although no judgment clearly states that recording and storage of photographs in a centralised system amounts to interference, applying the arguments raised in the previous cases by analogy, it is implied that once registered in a centralised scheme, that systematic storage amounts to interference.

In view of the above, the collection and storage of information interfere with the right to private life. Factors, such as the manner in which the data was collected (intrusive or covert) and the subsequent use of the data, have no bearing in finding any interference. However, in Weber v Saravia v Germany, the Court made another interesting remark; it held that the transmission of data to other authorities and the subsequent use by them enlarges the group of individuals with knowledge of the personal data intercepted and can therefore lead to investigations being instituted against the persons concerned. In the Court’s view, this danger amounts a further

---

252 ibid ¶81.
253 ibid ¶84.
254 ibid ¶85. The Court’s pronouncements mark a significant revisiting of its previous case law on this matter. In Kinnunen v Finland, the Court considered that fingerprints and photographs retained following the applicant’s arrest did not amount to an interference with their privacy ‘as they did not contain any subjective appreciations which called for refutation’. Kinnunen v Finland. Appl no 18291/91 (Commission Decision, 13.10.1993). Also see McVeigh v UK (1983) 5 EHRR 71.
256 Friedl v Austria (n218); Murray v UK (1995) 19 EHRR 193.
257 Kabera Karanja (n29) 94.
258 PG and JH v UK (n185).
259 Kopp v Switzerland (n232).
261 ibid ¶79.
4.5 Justification of interference under Article 8(2) ECHR

4.5.1 The ‘in accordance with law’ requirement

After determining that Article 8 ECHR applies, the next step is to examine whether a measure or action is ‘in accordance with law’. This criterion entails a two-step approach, whereby first it needs to be verified that the principle of legality is respected (in other words, that there is some sort of legal basis for the interference) and, secondly, that the law bears two essential qualities: adequate accessibility and sufficient precision. This criterion echoes the protection of the rule of law as ‘it proscribes any interference with rights save in relation to a set of knowable norms, which are not applied arbitrarily, but in sufficiently predictable fashion to give them the character of law at all’. In particular, the accessibility requirement means that the person concerned must be able to have an adequate indication of the legal rules applicable to a given case. This condition is thus fairly easily complied with if the legislation in question is based on legal texts that have been duly published. Sufficient precision is understood as allowing the person concerned, if need be with appropriate advice, to foresee, to a reasonable degree depending on the circumstances, the consequences that a given action may entail. Absolute certainty is not required.

In evaluating the foreseeability criterion, the Strasbourg Court has developed an elaborate catalogue of precise requirements. In Rotaru v Romania, the Court pointed out that the domestic legislation in question did not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as

---

262 ibid. Emphasis added.
263 Reference to the rule of law was explicitly made in Malone (n211), where in ¶67, the Court held that this requirement does not merely involve the existence of a legal basis, but also ‘quality of law’ requiring it to be compatible with the rule of law.
264 Sunday Times v UK (1992) 14 EHRR 229 ¶49.
265 ibid.
266 ibid.
267 Leander v Sweden (n212) ¶50-1.
gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. The law did not specify limits on the age of information held or the length of time for which it may be kept, and did not include provisions regarding the authorised persons to consult the files, the procedure to be followed or the use that may be made of the information thus obtained. In addition, although the law allowed interferences necessary to prevent and counteract threats to national security, the grounds for allowing such interferences were not laid down with sufficient precision. The existence of a supervisory mechanism and adequate and effective safeguards were also listed among the criteria for determining compliance with the ‘in accordance with law’ criterion. Overall, there must be a measure of legal protection in domestic law against arbitrary interferences with privacy by public authorities.

In Zakharov v Russia, a case involving the operation of a system of secret interception mobile telecommunications, the ECtHR elaborated further on these guarantees. In relation to the storage of intercepted data, the need for deletion of irrelevant data was pointed out. Another important proclamation of the Court was that in order for authority to authorise surveillance, there must be reasonable suspicion against the person concerned, understood as ‘factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures [...]’. As the Article 29 DPWP has pointed out, this proclamation seems to suggest that ‘only targeted data collection should be allowed’.

Finally, an interesting argument regarding the foreseeability requirement was advanced in Kennedy v UK, where the applicant claimed that the term ‘serious crime’ as set out in the British act in question was not sufficiently clear. In this regard, the Court opined that as long as the term is further clarified in the interpretative provisions of the contested act and the act itself, the foreseeability requirement would be met.

268 Rotaru v Romania (n212) ¶57. See Amann v Switzerland (n210) ¶68; Huvig v France (1990) 12 EHRR 528 ¶35.
269 ibid.
270 ibid ¶58.
271 ibid ¶59.
272 Zakharov v Russia 39 BHRC 435.
273 ibid ¶255.
274 ibid ¶260.
275 Article 29 DPWP, ‘Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)’ (WP237, 2016) 8.
277 ibid ¶159.
4.5.2 The existence of a legitimate aim

After assessing whether the interference is in accordance with the law, the next step is to determine whether the measure in question pursues one of the explicitly enumerated aims of Article 8(2). These aims are not defined, nevertheless the ECtHR recognises a wide margin of discretion to signatory States. As a result, it has rarely found a violation of Article 8(2) on the basis of this standard. Overall, the existence of a legitimate aim must be assessed at the time when the contested measure of activity takes place, signifying that an ex post evaluation is not permitted.

4.5.3 The proportionality test

The last step of assessing whether an impugned measure violates Article 8 ECHR or not is to evaluate whether its means are within the boundaries of what is necessary in a democratic society. In *Silver v UK*, the ECtHR clarified that the interference must correspond to a ‘pressing social need’ and be ‘proportionate to the legitimate aim pursued’.

In essence, the Court’s aim is to strike a balance between the interest of the society at large and the need to protect the individual’s human rights. At the heart of the Court’s jurisprudence is the doctrine of margin of appreciation. Overall, States enjoy a wide margin of appreciation as an expression of judicial self-restraint and as recognition of the principle of the choice of means. At the same time, the exceptions provided for in Article 8(2) must be interpreted narrowly. The scope of this margin is dependent upon the nature and seriousness of the interests at stake and the gravity of the interference. As indicated in *Rasmussen v Denmark*, the scope of appreciation will vary according to the circumstances, the subject matter and its background. In any case, as Greer points out, there is broad consensus on the correlation between the margin of discretion granted to States, the nature of the right in question and the

---

280 Z v Finland (n227) ¶75.  
281 *Silver v UK* (1991) 13 EHRR 582.  
282 ibid ¶7.  
284 *Handyside v UK* (1979-80) 1 EHRR 737 ¶48.  
286 Z v Finland (n227) ¶99; *Peck v UK* (n185) ¶77.  
288 ibid ¶40.
seriousness of the interference; the closer to the core of private life a measure affects, the narrower the margin of appreciation will be.

In relation to measures involving the collection and further processing of personal data for counter-terrorism purposes, the Court has granted a wide margin of appreciation to States. In Klass v Germany, the Court affirmed that States may not, in the name of fighting terrorism and espionage, adopt whatever measure they consider appropriate, but found that the guarantees provided by the German law at stake were strict enough to justify the interference with Article 8 ECHR. In Leander v Sweden, the Court recognised that the margin of appreciation ‘will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved’. For the purpose of safeguarding national security, the Strasbourg Court accepted that States need empowering legislations that enable the collection, storage and use of information, which, however, must be counter-balanced with procedural guarantees. However, it was careful to flag up ‘the danger […] of undermining or even destroying democracy on the ground of defending it’ and affirmed that for the purposes of fighting espionage and terrorism, Member States may not enact ‘whatever measures they deem appropriate’. Terrorism as a ‘special’ criminal offence enlarges the margin of appreciation of States. Irrespective of the instrument in place, even if it involves surveillance against individuals, the ECtHR found that adequate and effective safeguards must be in place. In MM v Netherlands, it held that ‘the greater the amount and sensitivity of data held and available for disclosure, the more important [is] the content of safeguards to be applied at the various crucial stages in the subsequent processing of the data’.

The ruling in S and Marper v UK is central for understanding how the Strasbourg Court addressed concerns related to the systematic collection and storage of biometric data of persons unsuspected of any crime. It marks the first case where the Strasbourg Court stepped into the mass data retention debate and condemned the blanket and indiscriminate collection and storage of sensitive information of individuals who were involved in criminal proceedings. The Court considered that the use of modern scientific techniques in the criminal justice system could not be allowed at any cost and without striking a fair balance between the potential benefits of the extensive use of such techniques and the private life interests. It was ‘struck by the blanket and

---

290 Leander v Sweden (n212) ¶59.
291 Klass v Germany (n210) ¶49.
292 Murray v UK (n236) ¶51.
indiscriminate nature of the power of retention’; factors such as the nature or gravity of the offence with which the individual was originally suspected, or their age, were irrelevant. The temporal character of retention was also an important element for the proportionality test. As the Court highlighted, the material could be retained indefinitely whatever the nature or seriousness of the offence. In addition, the law provided only for limited possibilities of removing the data from the system and there was no provision regarding the independent review of the justification for the retention on the basis of pre-defined criteria, such as the seriousness of the offence, previous arrests, the strength of the suspicion against the person concerned or any special circumstances.

Another important finding was the unequivocal rejection of the UK Government’s submission that the retention per se would have no direct or significant bearing on the applicants unless or until a match in the database would implicate them in the commission of a crime. The Court’s response is striking:

‘[T]he mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of data.’

Importantly, the Strasbourg judges explored the relationship between the legislation in question, and the presumption of innocence. In this respect, they observed the stigmatising effect that retention of data in centralised databases may have on the individual concerned:

‘Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the positions of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. In this respect, the Court must bear in mind that the right of every person under the Convention to be presumed innocent includes the general rule that no suspicion regarding an accused’s innocence may be voiced after his acquittal [...]. It is true that the retention of the applicants’ private data cannot be equated with the voicing of suspicion. Nonetheless, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while

---

294 S and Marper (n194) ¶119.
295 ibid. Also see ¶107.
296 ibid.
297 ibid ¶121. Emphasis added.
the data of those who have never been suspected of an offences are required to be destroyed.\textsuperscript{298}

The risk of stigmatisation is all the more alarming in cases involving minors due to their special situation and the importance of their development and integration into society.\textsuperscript{299}

In light of the above, the Court found that the retention of biometric material, including fingerprints, failed to strike the right balance between the competing interests and that the UK Government had overstepped any tolerable margin of appreciation.\textsuperscript{300}

The ECtHR did not rule out the collection of samples and fingerprints from suspects and their use during criminal investigations, or even their immediate deletion after they have been cleared out,\textsuperscript{301} but it sent a clear message to national authorities by placing significant limitations on States’ practices. The retention of data as such, particularly of sensitive ones, is not an insignificant process as it delineates between those individuals who are innocent and those who are not, and leads to stigmatisation and discrimination.\textsuperscript{302} Depending on the modalities of this retention, particularly the existence of corrective rules, the risk of stigmatising the individuals whose information is stored may become acute. In this respect, the Court emphasised that the presumption of innocence requires a differentiated treatment of data of individuals who have been convicted of an offence and those who have not.\textsuperscript{303} Therefore, key elements to be taken into consideration when designing retention mechanisms are: a) a distinction between serious and less serious offences; b) the age of the suspects; c) possibilities to have the data removed from the databases; d) independent review of the justification for the retention in accordance with pre-defined criteria; and e) limited retention periods.\textsuperscript{304}

Overall, \textit{S and Marper} demonstrates the Court’s growing awareness and sensitivity towards evolving technologies and the risk resulting from the collection and retention of personal data in sophisticated databases.

\textsuperscript{298} ibid ¶122.
\textsuperscript{299} ibid ¶124.
\textsuperscript{300} ibid ¶125.
\textsuperscript{301} Heffeman (n249) 503.
\textsuperscript{302} Valsamis Mitsilegas, \textit{The Criminalisation of Migration in Europe} (n8) 41.
\textsuperscript{303} Boehm (n32) 62; Hijmans notes ‘A database that is based on discriminatory processing is subject to a strict scrutiny, if the processing could lead to stigmatisation’. Hijmans (n91) 219.
\textsuperscript{304} Bellanova and De Hert (n269) 112.
5. Judicial assessment of privacy: The CJEU as the ‘unlikely hero of data privacy in Europe’

5.1 The interplay between data protection and privacy – Conceptual clarifications and the centrality of privacy

5.1.1 Pre-Lisbon

As early as 1980, the then ECJ was asked to interpret Community rules in light of Article 8 ECHR. In a series of judgments, it recognised the right to private life, as deriving from the common constitutional traditions of the Member States, as one of the fundamental rights protected by the legal order of the then Community. The enactment of EC/EU legislation in the field of data protection resulted in a proliferation of judgments pronounced by the Court dealing with various aspects of the elaborate data protection framework, most notably the Data Protection Directive. However, in the early days of the EUCFR’s life, the Court was reluctant to make direct references to either of its Articles and concentrated on privacy as enshrined in Article 8 ECHR. Promusicae marked a noteworthy shift in the Court’s reasoning in that it acknowledged the existence of the right to the protection of personal data, regarded as the right that ‘guarantees protection of personal data and hence of private life.’ Another case worth mentioning here is Rijkeboer. Although the Court made no reference to the Charter, it emphasised the intertwining between the Data Protection Directive and the right to privacy. The Court highlighted that the right is mentioned in Article 1 of that Directive and noted that its importance had been insisted upon in its


308 Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU [2008] ECR I-00271.

309 Ibid ¶ 63.

310 Case C-553/07 College van burgemeester en wethouders van Rotterdam v M E E Rijkeboer [2009] ECR I-3889.
case law. In the Court’s view, that right entailed that data must be accurate, processed in a correct and lawful manner, and disclosed to authorised persons.

### 5.1.2 Post-Lisbon

A significant jurisprudential moment concerning the analytical pattern followed by the Luxembourg Court is the ruling in *Schecke* regarding the validity of an EU provision on the finances of agricultural policy mandating the online publication of personal data of beneficiaries of EU funds. It was a first-class opportunity for the Court to clarify the perplexing interplay between privacy and data protection, since the referring Court considered the obligation contrary solely to the right to personal data protection. The CJEU found that both Articles 7 and 8 EUCFR were applicable; firstly, it noted that the right to the protection of personal data was enshrined in Article 8(1) EUCFR. This pronouncement is rather confusing because it seems that the Court considered the second and third paragraphs define the conditions for any limitation to the right to be regarded as lawful. Furthermore, it suggests that the Court transplanted the ECHR structure to the Charter, thus supporting the prohibitive approach to data protection. However, the Court opined that Article 8(2) EUCFR establishes the conditions for authorised processing. In addition, it suggested that both rights were subject to the limitations set forth by Article 52(1) EUCFR. Secondly, it regarded them as ‘closely connected’ to each other to the point of cumulatively forming a hybrid ‘right to respect for private life with regard to the processing of personal data’. The Court thus appears to nurture the idea that the right to the protection of personal data cannot operate on its own. The overarching right to be protected remains the privacy of the individual, however, since the interference takes place in the specific framework of personal data processing, data protection law also becomes of direct relevance. The Court’s approach

---

311 ibid ¶46-7.
312 ibid ¶49.
315 ibid ¶49.
316 ibid ¶50. Compare to the judgment in Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* (24.11.2011).
317 ibid ¶52. This approach is not as novel as one might think; See Article 1 of Regulation 45/2001 (n100) and Article 1(1) of the e-privacy Directive (n100). In this context, the Court did no more than to follow and generalise the approach taken by the EU legislator.
318 Tzanou (n31) 67.
thus supports the argument that data protection is to be understood as a right to support and enhance the protection of privacy in the specific context of data processing, but not as a *lex specialis*. This merging is confirmed by the Court’s statement that ‘the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention’.319

The importance of privacy was further manifested in *Schwarz*,320 a case concerning the validity of an EU rule requiring the mandatory collection of two fingerprints and their subsequent storage (at least) within EU passports.321 This case was another chance for the Court to elaborate on the relationship between privacy and data protection, as both the referring Court and AG Mengozzi assessed the Regulation in terms of the right to personal data protection.322 The Court provided a joint and simultaneous assessment of whether the provisions in question constituted a ‘threat to the rights to respect for private life and the protection of personal data’ and whether this twofold threat was justified. Then, in line with previous judgments, it linked the ‘provided in law’ condition as enshrined in Article 52(1) EUCFR and the ‘in accordance with law’ condition of Article 8(2) ECHR, with the requirement that personal data cannot be processed except on the basis of the consent of the person or some other legitimate basis laid down by law as set out in Article 8(2) EUCFR.323 In this framework, it proceeded to a joint examination of Articles 8(2) and 52 EUCFR considering Article 8 ECHR and the respective case law of the Strasbourg Court.324 While this approach has been criticised as containing ‘an alarming series of ungrounded shortcuts’325 it indicates: a) the ambiguity regarding the true content of Article 8 EUCFR; b) the inability of data protection law to operate as a fully-fledged fundamental right without having recourse to privacy; c) the overlap of data protection principles with privacy requirements; and d) the strong commitment of the Court to faithfully apply the ECtHR standards in the field of data processing.

---

319 Schecke (n313) ¶52.
320 Case C-291/12 Schwarz v Stadt Bochum (17.10.2013).
322 Case C-291/12 Schwarz v Stadt Bochum (17.10.2013) Opinion of AG Mengozzi. Advocate General’s approach raises two interesting issues; first, that the right to protection of personal data was enshrined in Article 8 taken as a whole (¶36-7); second, cross-references to the case law of the ECtHR were made (¶39). His approach can be seen as an attempt to disconnect the rights and consider Article 8 EUCFR as *lex specialis* in the field of communications and technology.
323 Schwarz (n320) ¶31-4.
324 ibid ¶27.
325 González Fuster, ‘Fighting For Your Right to What Exactly?’ (n314) 270.
In Digital Rights Ireland, the CJEU annulled the Data Retention Directive which required the retention en masse of telecommunications data. The judgment commenced with the Court assessing the existence of interferences with the rights to privacy and data protection on a separate basis. It followed the same approach also with regard to the requirement that an interference must respect the essence of the right. Then, for the proportionality test, it proceeded to a combined reading of the two rights. Therefore, whilst not referring to the hybrid right to ‘private life with regard to the processing of personal data’ as was pursued in previous judgments, its analysis eventually followed the same analytical pattern. Key in this respect is the Court’s pronouncement that the data protection has an important role in the light of the right to private life. Thus, despite the initial disentanglement of the rights half way through the judgment, the interferences were assessed in a unitary manner. As for the function of the right to personal data protection, the Court seems to consider it as one of the factors delimiting the margin of discretion enjoyed by the EU legislator. This subsidiary role of data protection was further declared by the Court, which held that ‘the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life’. As González Fuster has pointed out, the Court seems to recognise that the importance of data protection derives from the fact that it is part of the right to private life.

Finally, in Schrems, the Grand Chamber was faced with the validity of the Commission’s adequacy decision regarding the EU-US data transfers under the ‘Safe Harbor’ Agreement. In this judgment, which marks the return of the hybrid right to privacy with regard to the processing of personal data, the Grand Chamber went a step forward, stressing that the Data Protection Directive ‘seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular their fundamental right to private life with regard to the processing of personal

---

326 Joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Ireland (08.04.2014).
328 Digital Rights Ireland (n326) ¶32 and 36.
329 ibid ¶39-40.
331 ibid.
332 ibid ¶53.
333 González Fuster, ‘Fighting for Your Right to What Exactly?’ (n314) 275.
334 Schrems (n105).
data, but also a high level protection of those fundamental rights and freedoms’.\footnote{ibid ¶39. Emphasis added.}

Both the right to private life and the right to the protection of personal data are important in this regard.\footnote{ibid.}

From the analysis above, one may deduce certain conclusions regarding the relationship between privacy and data protection, and, importantly, about the role of privacy in evaluating cases involving the processing of personal data. Firstly, it is evident that the CJEU is striving to comprehend the content of the right to the protection of personal data and apply its reasoning in a consistent manner. In different judgments, the Court has found that the right is encompassed in Article 8(1) EUCFR, thus seemingly adhering to the prohibitive approach to data protection, whilst in Digital Rights Ireland it suggests that the core of the right is to be found in all three paragraphs. The Court seems to hover between the two approaches, however, even in cases where it appears to foster the prohibitive notion, which equips the right with a negative obligation, the understanding of the relationship between privacy and data protection, whereby the latter is meant to support and enhance the protection of the former, is consistent. These findings confirm my position that Article 8 EUCFR cannot and should not operate as a self-standing right. Furthermore, the Court has emphasised in multiple ways – one of which is the formation of a hybrid right to the private life with regard to the processing of personal data – that the underlying value to be protected is that of privacy, with the right to the protection of personal data being considered important as to reinforce the privacy protection, rather than to substitute it. Even in cases where the referring Court had not referred to the right to private life, the Luxembourg Court has added privacy into the equation and kept coherence and continuity with the ECHR. Therefore, the hierarchical relationship and complex entanglement between the two rights as flowing from the ambiguities and limitations surrounding data protection seems to be reflected in the case law of the Luxembourg Court.\footnote{Albeit with criticism See Kranenborg, ‘Article 8’ (n124) 260-2; Orla Lynskey, ‘From Market-Making Tool to Fundamental Rights: The Role of the Court of Justice in Data Protection’s Identity Crisis’ in Serge Gutwirth and others (eds) European Data Protection: Coming of Age (Springer 2013); Hustinx (n92) 20-3; Juliane Kokott and Christoph Sobotta, ‘The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR’ (2013) 3(4) International Data Privacy Law 222; Gonzalez Fuster, ‘Fighting for Your Right to What Exactly?’ (n314).}

Over the course of time, this approach has enabled the Court to provide a high level of privacy protection to individuals on a series of landmark judgments, and develop an elaborate checklist of markers that need to be assessed. The next section provides a codification of these
characteristics of privacy. For the purposes of this thesis, three judgments are of particular relevance; *Schwarz*, *Digital Rights Ireland* and *Schrems*.

5.2 Key characteristics of privacy protection

5.2.1 The judgment in *Schwarz* – Problematising the storage of fingerprint data

a) Legal and factual background

The case of *Schwarz* is the counterpart of the EChr ruling *S and Marper* in the jurisprudence of the CJEU. Its legal background could be summarised as follows: after 9/11, the US anti-terrorism legislation required nationals of countries under the US Visa Waiver Programme to hold machine-readable passports in order to visit the country. Under US pressure, in the Thessaloniki meeting of June 2003, the European Council called for ‘a coherent approach […] on biometric identifiers’. Regulation 2252/2004 was adopted concerning the security features and biometrics in passports and travel documents issued by Member States. Its Article 1(2) mandates the inclusion in all passports and travel documents of a storage medium containing a facial image and two fingerprints. Mr Schwarz, a German national, applied for a passport, but refused to have his fingerprints taken. Upon rejection of his application, he brought an action before the referring court requesting the issuance of a passport without taking his fingerprints, as this amounted to an interference with his right to personal data protection.

b) The Court’s ruling

The Court found that the EU Regulation met the fundamental rights standards as set out in Articles 7 and 8 EUCFR. However, it put forward some important findings that provide guidelines for the assessment of immigration databases. First, it clarified that since EU citizens are required to own a passport and they are not allowed to object to the processing of their fingerprints, they cannot be deemed to have consented to the collection and storage of their fingerprints. In considering the justification of the

339 Biometric Passports Regulation (n321).
340 *Schwarz* (n320) ¶32.
interference with privacy and data protection, the Court found no difficulty in asserting that the limitation was ‘provided for by law’; it was merely satisfied by the existence and publication of the Regulation without further examination of its provisions.\(^\text{341}\) It also easily tackled the question of whether the Regulation respected the essence of the fundamental rights in question and pursued an objective of general interest of the EU; the prevention of illegal entry to the EU qualified as a legitimate aim.\(^\text{342}\)

The bulk of the judgment is devoted to the assessment of the proportionality of the storage of fingerprints in EU passports. In this respect, the CJEU considered the storage of fingerprints an appropriate means of preventing the falsification of passports and facilitating the work of national authorities.\(^\text{343}\) The argument that fingerprint identification is subject to a not insignificant rate of false identification, or false non-identification (FRR or FAR),\(^\text{344}\) was dismissed by the Court. Although it recognised that this method is not flawless, it found it sufficient that it reduces the likelihood of admitting persons that should not be admitted.\(^\text{345}\) Crucial in the assessment was the fact that a possible match would not entail the automatic refusal of entry to the EU, but would merely draw the attention of authorities to that person resulting in a more detailed check in order to definitely establish their identity.\(^\text{346}\) Furthermore, the Court opined that the taking of two fingerprints could not be considered an operation of an intimate nature or causing any particular physical or mental discomfort.\(^\text{347}\) Besides, the Court was satisfied with the fact the Regulation required the collection of merely two fingerprints.\(^\text{348}\) The fact that both a facial image and fingerprints were stored was also deemed as not a priori giving rise in itself to a greater threat of fundamental rights.\(^\text{349}\) Then, by quoting \textit{S and Marper}, the Court held that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder.\(^\text{350}\) Therefore, any other form of storing those fingerprints is not provided, thus the regulation should not be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for their use for purposes other than the prevention of illegal entry into the EU.\(^\text{351}\)

\(^{341}\) ibid ¶35.
\(^{342}\) ibid ¶36-9.
\(^{343}\) ibid ¶41.
\(^{344}\) ibid ¶42.
\(^{345}\) Ibid ¶43.
\(^{346}\) ibid ¶44.
\(^{347}\) ibid ¶48.
\(^{348}\) ibid.
\(^{349}\) ibid ¶49.
\(^{350}\) ibid ¶56.
\(^{351}\) ibid ¶60-1.
On first reading, the Court’s reasoning may come as a disappointment to those preaching against the generalised application of biometric identities due to possible false matches. The EDPS has long warned about the risks pertained to the use of biometrics as unique means of identification, particularly in view of the tendency of authorities to overestimate the reliability of biometrics data.352 The judgment clarified that these limitations attached to the reliability of biometric identifiers do not necessarily mean that their collection and further processing is completely ‘off the table’. On second reading, the Court provided important guidance as to the criteria to be taken into consideration when balancing between the competing interests, thus setting important limits to state power to collect and use personal data for border control purposes. Firstly, significant importance is placed on the consequences of a possible false match. Privacy as dignity is thus placed at the centre of the Court’s approach. The impact of a false identification on the individual is qualitatively different when it involves a second round of checks on behalf of national authorities from possible implications in criminal investigations. Secondly, the compatibility of the Biometric Passports Regulation with fundamental rights was largely based on the finding that fingerprints are stored solely within the passport itself, which belongs to the holder alone.353 This is an important pronouncement as it raises serious questions regarding compatibility of the blanket and multi-purpose collection and storage of personal data.354 In fact, the judgment leaves wide leeway to argue a contrario that the centralised storage of fingerprints in massive databases is a disproportionate means of addressing immigration control prerogatives. Finally, another element for consideration is the fact that the Court favoured the storage of two fingerprints only, which also raises the question of whether a provision mandating the collection, storage and further processing of a full set of fingerprints would be equally considered proportionate.


353 Schwarz (n320) ¶60.

5.2.2 The judgment in *Digital Rights Ireland* – ‘A new hope’ for privacy

**a) Legal and factual background**

The first half of 2014 was marked by the release of two landmark judgments in *Digital Rights Ireland*[^355] and *Google v Spain*,[^356] in what has been eloquently described by Peers as a ‘privacy spring’.[^357] In *Digital Rights Ireland*, the CJEU in its most authoritative configuration, the Grand Chamber, declared the Data Retention Directive invalid. But the annulment of the Directive is only the climax of this story.

Let us start from the beginning. The Data Retention Directive was a surveillance-oriented measure adopted in the aftermath of 9/11 and particularly under the influence of the Madrid and London attacks. In a nutshell, it obliged the providers of publicly available electronic communications services or of public communications networks to retain various types of telecommunications data – the so-called metadata – by all individuals within the EU, ‘in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime’.[^358] Metadata are data about the location (source and destination), date, time and duration, as well as data to identify the type of communication and equipment used, in other words, they are ‘data about data’. Whereas the Directive obliged service providers to retain telecommunications data, the modalities of law enforcement access to the data were to be determined through implementation at the national level. For that reason, it was adopted under an internal market legal basis rather than a former third pillar one.[^359]

Unsurprisingly, the Directive generated significant controversy and in 2006 it was challenged before the Luxembourg Court on legal basis grounds, but survived the judgment.[^360] The Court accepted that the internal market legal basis was the correct one, as the instrument enabled the elimination of obstacles in the internal market even

[^355]: Digital Rights Ireland (n326).
[^356]: Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (13.05.2014).
[^358]: Data Retention Directive, art 1(1).
though the ultimate purpose of data retention was to facilitate police action.\textsuperscript{361} Crucial in its assessment was the fact that the Directive did not govern access by law enforcement authorities.\textsuperscript{362} Nevertheless, the Court inserted a small caveat; it explicitly mentioned that it had not approved the compatibility of data retention with the fundamental right to privacy.\textsuperscript{363} As Boehm has rightly pointed out, the Court drew a line between the retention and the storing of the data, and its subsequent use and access.\textsuperscript{364}

At the national level, the revolt by domestic constitutional courts was massive; the Bulgarian, Romanian, German, Cypriot and Czech constitutional courts struck down their respective laws implementing the Directive.\textsuperscript{365} In particular, the Bulgarian Constitutional Court first declared the unconstitutionality of the legislation transposing the directive, at least in part, due to lack of privacy guarantees and the lack of sufficient limitations concerning access to the retained data.\textsuperscript{366} The Romanian Constitutional Court annulled the transposing law in its entirety for violating a series of rights entrenched in the national Constitution, namely the right to privacy, inviolability of domicile, secrecy of communications and the right to free development of human personality.\textsuperscript{367} Key in its ruling was that the \textit{blanket retention} of data was deemed disproportionate \textit{by nature} irrespective of its subsequent use.\textsuperscript{368} The German Constitutional Court found the national implementing law to be in fundamental breach

\textsuperscript{361} ibid ¶63–64.
\textsuperscript{362} ibid ¶80.
\textsuperscript{363} ibid ¶57.


\textsuperscript{368} In particular, the Court found unconstitutional ‘the legal obligation with a \textit{continuous character}, generally applicable, of data retention. This operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to \textit{overturn the presumption of innocence and to transform a priori all users} of electronic communication services or public communications networks \textit{into people suspected of committing terrorism crimes or other serious crimes}.’ Emphasis added.
of Article 10(1) of the German Constitution devoted to the privacy of correspondence and telecommunications.\(^{369}\) Similarly, the Cypriot Constitutional Court considered the transposition provisions to violate both privacy and the secrecy of communications.\(^{370}\) As for the Czech Constitutional Court, it expressed its doubts on whether an instrument of global and preventive retention of metadata on almost all electronic communications may be deemed necessary and adequate in view of the intensity of the intervention to the private sphere of an indefinite number of persons.\(^{371}\)

Against this – arguably heated – background, the CJEU was called to rule on two requests for preliminary rulings; one emanating from the ‘Digital Rights Ireland’, an NGO that challenged before the Irish High Court the compatibility with fundamental rights of the Irish implementing law, and a second stemming from a ‘class action’ brought before the Austrian Constitutional Court by more than 11,000 Austrian citizens against parts of the Austrian transposing legislation. Both referring Courts inquired into the validity of some provisions of the Directive in light of both the rights to private life and to the protection of personal data, as well as the freedom of expression.

**b) The Court’s ruling**

From the outset, the Court observed that the data retained made it possible to know the identity of the person, with whom the data subject had communicated, and the form, time, place and frequency of communications.\(^{372}\) In the Court’s view, this data set ‘taken as a whole’:

‘may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them’.\(^{373}\)

---


\(^{372}\) Digital Rights Ireland (n326) ¶26.

\(^{373}\) ibid ¶27. Advocate General eloquently points out in this respect: ‘There are, however, data which are in a sense more than personal. These are data which, qualitatively, relate essentially to private life, to the confidentiality of private life, including intimacy. In such cases, the issue raised by personal data
Having made this remark, the CJEU found no difficulty in asserting that the retention of telecommunication data amounted to an interference with Article 7 EUCFR as it ‘derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic telecommunications sector’.  

The Court recalled that the existence of an interference is not affected by the sensitivity of the information on the private lives, or a possible inconvenience in any way of the persons concerned. Furthermore, in line with the case law of the ECtHR in Leander v Sweden, Rotaru v Romania and Weber and Saravia v Germany, the Court contended that access by the competent national authorities to the data constitutes a separate interference with privacy. The Grand Chamber found it even easier to declare an interference with the right to protection of personal data simply ‘because [the directive] provides for the processing of personal data’.

The next step for the Court was to declare that the interference is wide-ranging, and must thus be considered to be particularly serious. This proposition was based on the fact that there is no requirement for the service providers to store the data to be retained within the territory of a Member State, under the jurisdiction of a Member State; a fact which considerably increases the risk that such data may be accessible or disclosed in breach of privacy standards. Furthermore, in line with the AG’s view, the Grand Chamber contended that the retention and subsequent use 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’.

---

374 ibid ¶32 and 34; Emphasis added. Ojasen rightly notes that the Court could have spelled out in a clearer manner that metadata may reveal much sensitive information about the individual, such as on health, religion and sexuality or regarding certain particularly sensitive relationships (e.g. lawyer-client). Tuomas Olasen, ‘Privacy is More than Just a Seven-letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance’ (2014) 10(3) European Constitutional Law Review 528, 535.

375 Digital Rights Ireland (n326) ¶33.

376 ibid ¶35.

377 ibid ¶36. Compare with Tzanou (n31) 129.

378 ibid ¶37.

379 Digital Rights Ireland, Opinion of AG (n373) ¶77, 80.

380 Digital Rights Ireland (n326) ¶37. The Advocate General’s views are enlightening in this regard. He found that the collection and retention in huge databases of large quantities of everyday telecommunication data establishes the conditions of surveillance. Although carried out only retrospectively when the data are used, the collection and retention constitutes a permanent threat to privacy throughout their retention period (¶72). Furthermore, in his view, ‘the vague feeling of surveillance’ may influence the right to freedom of expression and information (¶52). His finding is in line with the views of the Romanian Constitutional Court (n367).
Next, the Court summarily dismissed the argument that the interference does not respect the essence of privacy and data protection. With regards to the former, it pointed out that the obligation imposed by the Directive does not permit the acquisition of knowledge of the content of the electronic communications *per se*.\(^{381}\) As for the right to personal data protection, the Court observed that the Directive requires the respect of certain data protection and data security principles.\(^{382}\) This narrow perception of the essence of the rights in question has been rightly criticised as ‘hierarchical and formalistic’, because it disregards that even metadata may reveal as much of someone’s personal circumstances as the interception of communications content, whereas a long retention period may enable the construction of ‘rich longitudinal metadata about a person’s activities over an extended period’.\(^{383}\) The Court equally found that the measure in question genuinely satisfied an objective of general interest, that is to say, public security.\(^ {384}\) In this respect, it highlighted Article 6 EUCFR, which sets out the right of any person not only to liberty, but also to security.\(^ {385}\)

The heart of the ruling is the proportionality test conducted by the Court under the requirements of Article 52(1) EUCFR. In this regard, by referring to the case law of the ECtHR, particularly in *S and Marper*, the Grand Chamber noted that the discretion the EU legislator enjoys is dependent upon a number of factors, such as the area concerned, the nature of the right in question, the nature and seriousness of the interference, and the object pursued by the interference.\(^ {386}\) Then, it declared that this discretion is reduced and, therefore, its review of that discretion should be strict in view of ‘the important role played by the protection of personal data in the light of the fundamental right to respect for private life’ and the extent and seriousness of the interference.\(^ {387}\) The appropriateness of telecommunications data retention was not called into question. It held that due to the growing importance of means of electronic communication, the retained data allow the competent prosecutorial authorities to have additional opportunities to shed light on serious crime, and, therefore, are a ‘valuable tool’ for criminal investigations.\(^ {388}\)

In relation to the proportionality of retention, however, the Grand Chamber enumerated a series of loopholes and inadequacies of the legislation by taking into

381 *Digital Rights Ireland* (n326) ¶39.
382 Ibid ¶40.
384 *Digital Rights Ireland* (n326) ¶41-2.
385 Ibid ¶42.
386 Ibid ¶47.
387 Ibid ¶48.
388 Ibid ¶49.
consideration arguments raised by the national constitutional courts. A close examination of the judgment reveals four areas touched upon by the Court; the personal scope of the Directive, the modalities of access and subsequent use of the data; the retention period; and data security.

Starting with the personal scope of the Directive, it pointed out that it involves all traffic data and applies to all means of electronic communication. As a result, it concluded that it practically affects the entirety of the European population. In addition, the Directive covers, in a generalised manner, all persons and all means of electronic communication, as well as traffic data without any differentiation, limitation, or exception being made. The Court exposed the absence of any relationship between the huge amount of retained data and persons likely to be involved in committing serious crimes. There was no requirement that the persons are even indirectly in a situation that is liable to give rise to criminal prosecutions. Instead, the Directive was applicable even to persons against whom there is no evidence that their conduct may be linked, even remotely or indirectly, to serious crime. Furthermore, the Directive did not include any exception concerning those persons whose communications are subject to professional secrecy, such as lawyers. Moreover, it contained no rules restricting the retention to: i) data pertaining to a particular time period, and/or a particular geographical zone, and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

The issue of access to the data by law enforcement authorities and their subsequent use was also thoroughly scrutinised. In this regard, the Grand Chamber was dissatisfied with the absence of any objective criterion determining the limits of the access and their subsequent use, as well as the lack of substantive and procedural conditions concerning this access. In particular, it made reference to the fact that there is no explicit rule asserting the access to, and use of, data involved merely the prevention, detection or prosecution of serious offences. To these deficiencies, it added the lack of definition of what constitutes a serious crime. Moreover, no rules delimiting the number of persons authorised to access, and subsequently use, the data to what is strictly necessary on the

390 Digital Rights Ireland (n326) ¶ 56.
391 ibid ¶57. Emphasis added.
392 ibid ¶58.
393 ibid ¶59.
394 ibid ¶60-1.
basis of the objective were included.\textsuperscript{392} Importantly, it set the threshold particularly high by requiring that prior to access by the competent national agencies, the conditions of access must be reviewed.

\textit{by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.}\textsuperscript{396}

The next issue examined by the Court related to the retention period, where it was noted that the prescribed retention period of at least six months did not differentiate between the distinct categories of data on the basis of their possible usefulness for the purposes of the objective pursued, or according to the persons concerned.\textsuperscript{397} Furthermore, given the fluctuating retention period due to national transposition, no remark was made that its determination at the national level must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.\textsuperscript{398}

Already at this stage, the Court had provided a first set of criteria that the EU legislator had failed to meet, leading it to conclude that the directive ‘entails a wide-ranging and particularly serious interference […] without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.’\textsuperscript{399} However, the Court’s assessment did not end there. A second set of rules specifically involving data security, ‘as required by Article 8 of the Charter’,\textsuperscript{400} was provided. In this regard, it was submitted that the Directive did not provide for sufficient safeguards against the risk of abuse and against any unlawful access and use of that data.\textsuperscript{401} In particular, the Directive lacked rules particularly adjusted to take into account: i) the vast quantity of data whose retention is required by that directive, ii) the sensitive nature of that data, and iii) the risk of unlawful access to that data. Furthermore, the Directive did not require the enforcement of technical and organisational measures that would ensure a particularly high level of protection and security, but permitted providers to take into consideration economic interests in setting

\textsuperscript{395} ibid \textsuperscript{¶}62.
\textsuperscript{396} ibid; Emphasis added.
\textsuperscript{397} ibid \textsuperscript{¶}63.
\textsuperscript{398} ibid \textsuperscript{¶}64.
\textsuperscript{399} ibid \textsuperscript{¶}65.
\textsuperscript{400} ibid \textsuperscript{¶}66. However, in the Court found this condition emanating from the case law of the ECtHR concerning the right to respect for private life, particularly \textit{Liberty v UK (n231) ¶}62-3 and \textit{Rotaru v Romania (n212) ¶57}. Indeed the risk of abuse and unauthorised access to the data stored necessarily implies a significant widening of the pool of persons who have access to the data.
\textsuperscript{401} ibid.
Moreover, the irreversible destruction of data after the retention period had expired was not ensured, as there was no obligation that the data would be retained within the EU. The final point of concern related to the existence of independent supervision, which was indeed explicitly mandated by Article 8(3) EUCFR, but was not expressly required by the Directive.

c) Post-Digital Rights Ireland: Privacy and pre-emptive surveillance

Undoubtedly, Digital Rights Ireland has already qualified as a landmark ruling ‘marking a constitutional moment in striking a balance between fundamental rights and security in the digital age’. In an era of proliferation of surveillance practices via the collection and further processing of a wide range of data, including sensitive data, the CJEU stepped into the surveillance turmoil and released a judgment that is a ‘decisive move towards using privacy to limit pre-emptive surveillance.

The Court’s proclamations cannot be overstressed.

Firstly, at a theoretical level, three layers of an interference with privacy can be discerned: the first layer is constituted by the initial collection and creation of data by telecommunication providers; the second layer emerges out of the obligation to retain the collected data; and the third layer relates to the further processing by law enforcement authorities by means of getting access to the data for countering terrorism and serious crime.

Secondly, the Grand Chamber pointed out that such practices must be understood as the EU enabling state surveillance of large numbers of persons on a constant basis. In finding that the interference with privacy is particularly serious, it took into account a series of characteristics pointed out by the AG: a) the lack of requirement to store the retained data within the EU; b) the lack of information which may lead to a feeling of being in a constant state of surveillance; and c) the retention and storage of everyday data of a very large number of persons in huge databases. Furthermore, highlighted the element of surveillance could be understood as the Court advancing the view that such a

---

402 ibid ¶67.
403 ibid ¶67–8.
404 ibid ¶68.
406 Mitsilegas, ‘The Transformation of Privacy’ (n134) 54.
serious interference has an adverse effect upon the overall relationship of trust between
the individual and the State. 407

Thirdly, despite accepting that the interference served a legitimate aim, the Grand
Chamber condemned practices entailing the blanket, massive and indiscriminate
retention of personal data for law enforcement purposes without the adoption of strict
safeguards.

As noted by Council Legal Advice Service:

‘[T]he Court will not satisfy itself with anything less than a strict assessment
of the proportionality of measures that constitute serious restrictions to
fundamental rights, however legitimate the objectives pursued by the EU
legislature. It also indicates that such measures do not stand a serious chance
of passing the legality test unless they are accompanied by adequate
safeguards in order to ensure that any serious restriction of fundamental
rights is circumscribed to what is strictly necessary and is decided in the
framework of guarantees forming part of Union legislation instead of being
left to the legislation of Member States.’ 408

Indeed, data retention as a form of preemptive surveillance is significantly different
from interception of communications content, whereby authorities request the
preservation of data concerning individuals suspected of crime. Key in this context is
that the retention involved a very large number of persons (even indefinite) who are a
priori unsusp...
alter this finding. The key element is the normative choice of surveying parts of the
everyday conduct of a very large group through the mandatory collection, storage and
further processing of personal data en masse without distinction, as opposed to targeted
forms of surveillance.

It is true that the Grand Chamber did not totally overrule mandatory data retention
as a weapon against terrorism and other serious crimes, and it is implied that some form
of data retention may potentially be compatible with fundamental rights. However, it
stepped up and defined a series of strictly circumscribed criteria that need to be taken
into consideration by the EU legislature. These points can be largely inferred from the
flaws of the Data Retention Directive that triggered its invalidation. In this sense, the
Court has established a form of dialogue between itself and the EU legislator in which
the Court does not only annul a legal instrument, but also provides instructions
regarding the design of valid data retention schemes that are respectful of fundamental
rights whilst accomplishing its stated aim. Although it takes up its role as the
guardian of the Charter very seriously, it equally transfers the responsibility for
fundamental rights to the EU legislator.

The judicial guidelines can be summarised as follows:

a) Generalised and indiscriminate data retention as a preventive surveillance
mechanism seems to be unacceptable, disproportionate and thus prohibited. Data
collection must be confined to situations which pose a threat to public security by
restricting the measure to a time period, to a geographical zone, or to groups of persons
likely to be involved in a serious crime, or more broadly to persons whose
communications may contribute to law enforcement.

b) Data retention periods must be defined on the basis of the data’s potential
usefulness and should remain as short as possible. During the retention of the data, a
high level of security must be ensured, including the control of an independent authority
and their location within the EU.

c) Ex post access and further processing of the data as a separate interference with
privacy should be subject to further requirements; it must be restricted to what is strictly
necessary and must respect procedural and substantive conditions. Access should be
limited to the purposes of preventing, detecting, and prosecuting well-defined serious
offences. Finally, requests for access should be conditional upon prior review by a court
or an independent administrative body entrusted with ensuring compliance with

413 Ojamen (n374) 541.
414 Granger and Irion (n383) 845.
constitutional and legislative limits to data processing. These guidelines serve a checklist of criteria for taking into consideration when assessing other mechanisms.

d) Data security and independent supervision must be ensured.

Overall, the judgment constitutes a strong vindication of privacy as a genuine fundamental right, the erosion of which is overruled even for the sake of pursuing highly valued objectives, such as counter-terrorism. It underlines the role of the CJEU as some form of a Constitutional Court whereby the review of fundamental rights by strictly scrutinising EU legislative measures becomes a central function. This constitutional role suggests a balancing between the powers of the EU and the Member States, and developing principles of judicial review. Furthermore, by placing such limits on generalised surveillance, the Grand Chamber seems to foster a concept of privacy intertwined with the values of personal autonomy, whereby individuals must be left to pursue their everyday activities, such as their personal communication, away from State intervention, unless there is suspicion of wrongdoing, and thus enjoy a certain degree of autonomy in their contemporary living that allows for self-development. Rather than enabling people to regain ‘control’ of their telecommunications data, Digital Rights Ireland prohibits such control to be taken by state authorities.

The Data Retention Directive generated legal chaos at the national level, as most Member States had put in place data retention obligations in fulfillment of the Directive. In the aftermath of the judgment, national retention schemes concerning telecommunication data could be legally based on the e-privacy Directive, but these States were confronted with the question of whether these obligations were compatible with that Directive as well as the rights to privacy and data protection. In this framework, two joined cases reached the CJEU that essentially enquired if a general obligation to retain telecommunication data is precluded, and if not, which safeguards must be out in place and what circumstances must be taken into account.

On 19 July 2016, AG Saugmandsgaard Øe delivered his Opinion. Taking Digital Rights Ireland a step forward, the AG raised two important points. Firstly, he took the

---

416 Granger and Irion (n 383) 844-5. On the role of the CJEU as a constitutional court see Paul Graig and Gráinne de Búrca, EU Law, Text, Cases and Material (5th edn, Oxford University Press 2011) 61-66.

417 Ibid 65.

418 See n100.

419 Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15).

420 Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), Opinion of AG Saugmandsgaard Øe. For a comment see Vanessa Franssen, ‘The Future of National
view that a general retention obligation may be proportionate only in relation to serious offences, as '[t]he considerable risks that such obligations entail outweigh the benefits they offer in combating ordinary offences and in the conduct of proceedings other than criminal proceedings.'\textsuperscript{421} This is a key finding in that it suggests that generalised surveillance mechanisms used for purposes other than the combating of terrorism and other serious crimes run the danger of being deemed disproportionate. Secondly, the AG highlighted the negative aspects of general retention schemes by focusing on the effects on the individuals concerned, whose communications are monitored even though ‘the vast majority of the data retained will relate to persons who will never be connected in any way with serious crime’.\textsuperscript{422} In this respect, he distinguished between ‘individual’ and ‘mass’ interferences, whereby the former corresponds to feelings of surveillance generated in the minds of individuals, and the latter affects a substantial portion of the population.\textsuperscript{423} He further provided examples on how telecommunication databases could reveal personal bids of individuals’ lives, such as psychological disorders or political opinions, on the basis of metadata,\textsuperscript{424} and observed that the risk of abusive access on the part of competent authorities is directly related to the use of the system, concluding that ‘[t]he risk of illegal access, on the part of any person, is as substantial as the existence of computerised databases is extensive.’\textsuperscript{425}

5.2.3 The judgment in Schrems – From the ‘Safe Harbor’ back into the (data transfer) storm

a) Legal and factual background

The last case of interest involves the transfer of personal data from the EU to the US on the basis of the EU-US Safe Harbor Commission Decision (Safe Harbour Agreement)\textsuperscript{426} which asserted that US data protection rules provide an adequate level of protection.\textsuperscript{427} In view of the Snowden revelations regarding the mass surveillance

\textsuperscript{421} ibid ¶172.
\textsuperscript{422} ibid ¶252.
\textsuperscript{423} ibid ¶253-6.
\textsuperscript{424} ibid ¶257-8.
\textsuperscript{425} ibid ¶259.
\textsuperscript{427} See above, Section 3.1.
conducted by the US NSA PRISM Programme, it became evident that the data transferred from the EU to the US could be accessed by the NSA in the course of mass, and indiscriminate, surveillance activities. Albeit acknowledging the incompatibility of the US practice with the EU privacy framework did not revoke its adequacy decision, as this would have adverse effects to the interests of the companies participating in the programme.\footnote{Commission, ‘Restoring trust in EU-US data flows’ (Communication) COM(2013) 846 final; ‘Functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU’ (Communication) COM(2013) 847 final.\footnote{Schrems (n105) ¶33.}}

Mr Schrems, an Austrian student and Facebook user, filed a complaint before the Irish Data Protection Authority requesting the prohibition of transfer of his Facebook data. The latter ‘washed off their hands’ and referred to the Commission adequacy decision. An action was brought before the Irish High Court which requested a preliminary ruling enquiring whether the national data protection authority had the power to dispute the Commission adequacy decision when examining a person’s claim, considering that the ‘mass and undifferentiated accessing of personal data’ by the NSA was clearly against Irish and, more generally, EU standards.\footnote{Case C-362/14 Maximilian Schrems v Data Protection Commissioner (20.10.2015) Opinion of AG Bot.\footnote{For an overview of the judgment, particularly its implications to transfer of EU data to the US see Rob Robert, ‘Safe Harbor – Is the EU Guilty of Double Standards?’ (2015) 16(2) Privacy & Data Protection 5; Rohan Massey, ‘The US-EU Safe Harbor Framework Is Invalid: Now What?’ (2016) 22(1) Computer and Telecommunication Law Review 1.\footnote{Schrems (n105) ¶40-1.}}}

**b) The Court’s ruling**

In line with the AG’s view,\footnote{Schrems (n105) ¶33.} the CJEU declared the Safe Harbor Agreement invalid,\footnote{Case C-362/14 Maximilian Schrems v Data Protection Commissioner (20.10.2015) Opinion of AG Bot.\footnote{For an overview of the judgment, particularly its implications to transfer of EU data to the US see Rob Robert, ‘Safe Harbor – Is the EU Guilty of Double Standards?’ (2015) 16(2) Privacy & Data Protection 5; Rohan Massey, ‘The US-EU Safe Harbor Framework Is Invalid: Now What?’ (2016) 22(1) Computer and Telecommunication Law Review 1.\footnote{Schrems (n105) ¶40-1.}} holding that the Commission had exceeded its authority in adopting Decision 2000/520, as it contained ‘national security’ derogations without necessary corresponding protections required under EU law. The Grand Chamber took a two-step approach; it first considered the powers of national supervisory authorities concerning claims that question the validity of adequacy decisions and then considered the content of the Commission adequacy decision.

Firstly, it considered the role and powers of national data protection authorities and placed emphasis on their independence, which is essential for the effective protection of individuals.\footnote{Schrems (n105) ¶40-1.} It found that the existence of an adequacy decision does not prevent them from considering claims lodged by persons whose personal data have been, or may be,
transferred to a third country.\textsuperscript{433} Whilst it clarified that until a Commission adequacy decision is withdrawn, annulled or declared invalid supervisory authorities may not adopt measures contrary to that decision, it gave clear guidelines as to how national supervisory authorities and courts are supposed to deal with claims. If, during the examination of the merits of a claim, they consider it unfounded, the applicant should be able to bring an action before national courts.\textsuperscript{434} National courts may then refer the matter to the CJEU for consideration. Conversely, if the objections advanced by the claimant are viewed as well founded, national supervisory authorities should be able to engage in legal proceedings pursuant to national law.\textsuperscript{435}

Taking into account its previous proclamations, the Luxembourg Court then scrutinised the adequacy decision itself, even though it had only implicitly been asked to. Whilst not referring to the NSA revelations as such, the concerns stemming from the possibility of mass surveillance on behalf of the US underpin the Court’s reasoning. Firstly, it required a particularly high threshold in relation to the transfers of data, by proclaiming that the requirement of adequacy should be understood as requiring the third country to ensure a level of protection ‘essentially equivalent’ to that guaranteed under EU law.\textsuperscript{436} Secondly, it affirmed that the adequacy decisions are subject to periodical review, particularly if evidence gives rise to doubts that the level of protection remains adequate.\textsuperscript{437} Of particular importance in this respect are any circumstances that may have arisen after the adoption of the decision.\textsuperscript{438} As in Digital Rights Ireland, the Court limited the margin of discretion afforded by the Commission as to the adequacy of the level of protection ensured by a third country on the basis of two factors:

‘first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and secondly, the large number of persons whose fundamental rights are liable to be infringed’.\textsuperscript{439}

Then, it expressed serious concerns stemming from the fact that the applicability of the Safe Harbor principles was subject to a broadly worded derogation related to national security, public interest and law enforcement reasons, which in fact superceded the obligations under EU law.\textsuperscript{440} As a result, national security requirements had primacy over the principles. The Court considered such general derogation as an interference

\begin{itemize}
\item \textsuperscript{433} ibid ¶53-6.
\item \textsuperscript{434} ibid ¶64.
\item \textsuperscript{435} ibid ¶65.
\item \textsuperscript{436} ibid ¶73.
\item \textsuperscript{437} ibid ¶76.
\item \textsuperscript{438} ibid ¶77.
\item \textsuperscript{439} ibid ¶78.
\item \textsuperscript{440} ibid ¶84-6.
\end{itemize}
with the fundamental rights of the persons whose personal data are transferred to the US.\textsuperscript{441} However, it found no provision limiting such interference or the existence of a judicial redress mechanism.\textsuperscript{442} Importantly, it opined that the limitation to privacy was not restricted to what is strictly necessary where legislation mandates:

‘on a generalised basis [the] storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail’.\textsuperscript{443}

In particular, it held that generalised access constituted an interference that compromises the essence of the right to privacy.\textsuperscript{444} This marks the first time that the Court found a type of processing affecting a fundamental right to its core.\textsuperscript{445} Furthermore, the lack of any effective remedies compromised the essence of the right to effective remedies enshrined in Article 47 of the Charter.\textsuperscript{446}

\textit{Schrems} has already made its way into the EU jurisprudential history as a privacy victory equivalent to the \textit{Digital Rights Ireland} ruling. In addition to the very important proclamations of the Court in relation to the role of national supervisory authorities and the application of a high threshold in relation to the term ‘adequate’,\textsuperscript{447} the Grand Chamber made some important remarks regarding mass surveillance practices. Drawing significantly from the data protection standards established in \textit{Digital Rights Ireland}, it clarified that mass surveillance is inherently and intrinsically unlawful. It expanded its proclamations on retention to explicitly cover other forms of processing, namely the storage of data. It is noteworthy that the wording of the Grand Chamber (storage and access on a generalised basis) is not as strong that the terminology used by the Advocate

\begin{flushleft}
\textsuperscript{441} ibid ¶ 7.
\textsuperscript{442} ibid ¶88-9.
\textsuperscript{443} ibid ¶93.
\textsuperscript{444} ibid ¶94.
\textsuperscript{445} Ojasen notes that ‘the Court even seems to acknowledge the idea that fundamental rights must be understood as having a ‘hard core’ that should remain outside the scope of application of the balancing test’. Tuomas Ojanen, ‘Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter – ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner’ (2016) 12(2) European Constitutional Law Review 318, 325.
\textsuperscript{446} ibid ¶95.
\end{flushleft}
General (‘generalised surveillance’, 448 ‘mass, indiscriminate surveillance’ 449 and ‘extremely serious interference’ 450). Furthermore, the Court ruled that generalised access to the content of communications compromises the essence of privacy. Practices, however, involving the indiscriminate storage of huge amounts of personal data from large groups of persons do not stand a chance to pass the EU proportionality test without strict safeguards. These involve not only the personal scope of surveillance which must be defined by taking into account different interests already at the stage of the storage of personal data, but also the conditions and purposes of access and subsequent use, which must be defined on the basis of objective criteria and subject to the principle of proportionality.

6. Conclusion

The aim of this Chapter was to provide the theoretical framework of the thesis by addressing two main issues:

1) The centrality of privacy in assessing instruments involving the collection, storage and further processing of personal data, such as EU immigration databases; and

2) The standards for compliance with the right to private life as drawn from the relevant case law of the Strasbourg and Luxembourg Courts.

From the outset, it was observed that privacy as a notion is not universally conceptualised and is attached to a multiplicity of other concepts and values, which, nonetheless, appear insufficient to adequately foster and frame the concept on their own. Depending upon context and jurisdiction, privacy can be anchored to a series of notions and values, particularly individual autonomy and dignity. In the field of personal data processing, the ECtHR has interpreted privacy in a constructive manner in order to safeguard its dynamic nature and flexibility. Under EU law, the right to private life has found legislative expression in the field of personal data processing via the adoption of a series of general and sectoral data protection instruments, striving in between elaborate, yet fragmentary, provisions and an internal market logic under which free flow of data must be ensured. At constitutional level, the coexistence of a right to privacy (Article 7 EUCFR) alongside a novel right to personal data protection (Article 8

448 Schrems, Opinion of AG (n431) ¶167.
449 ibid ¶200
450 ibid ¶171.
EUCFR) raises questions in relation to the interplay between the two rights, not least regarding the appropriate lens through which legal instruments regulating different instances of personal data processing must be assessed.

The spectrum of approaches is perhaps as wide as the number of scholars; from skeptics towards the elevation of data protection to the status of a fundamental right to those considering it an overdue development, and from those making a case for its complete surrender to privacy to those calling for their separation and the independent operation of each concept. Some authors have resorted to depictions of their correlation by reference to the bonds enjoyed by family members: Safjan considers data protection as an unwanted child; Tzanou parallelises the relationship between privacy and data protection by using the Ancient Greek myth of the birth of Athena from the head of Zeus; and Boehm supports the idea that data protection and private life are twins, but not identical. Building on Boehm’s depiction, this study understands the relationship between the two rights as one shared by inseparable conjoined twins, whereby privacy and data protection share the same main organs, which are situated within the privacy ‘body’, but data protection seems to have lacked in development. This Chapter demonstrated that although data protection law is relatively considered as more straightforward than privacy, the nature, scope and role of the right are far from unproblematic. In my view, the prevailing view on data protection portrays a right that is rather weak on its own. By contrast, the right to private life, due to its inherent flexibility and robust obligations that its protection entails, provides a more holistic framework for addressing concerns in relation to the processing of personal data. It enables a focus on the individual in question and the effect of an instrument in their contemporary life, rather than concentrating on the protection of specific categories of personal data. It can further challenge the justification and practices of collecting personal data as such, rather than merely imposing the ‘rules of the game’.

Hijmans claims that it is unimportant to distinguish between privacy and data protection when assessing legislative measures concerning the processing of personal data, and that both rights should be considered as part of one system. This study considers that since the constitutional entrenchment of the right to the protection of personal data has generated a trend among scholars to focus on its potential without recourse to the right to private life, the centrality of privacy should be highlighted. The

452 Tzanou (n31) 11.
453 Boehm (n32) 4.
454 Hijmans (n91) 63-72.
effectiveness of data protection law is undermined by its specific mandate as a transparency tool that may not question normative legislative choices. Relying solely on data protection may in fact lead to the opposite effect from the one intended; data protection may transform from a reinforcing and progressive instrument into a repressive weapon. Therefore, not distinguishing between the two rights seems a sensible solution and is in line with the approach of the European Courts, but only to the extent that the hierarchical relationship between the two rights is not called into question. Data protection law is a specification of the right to private life in the field of information technology, in that it regulates different aspects of processing of personal data, but it should not be considered as *lex specialis*. The right to private life should, therefore, remain in the spotlight as the appropriate framework for assessing issues stemming from the processing of personal data, and the data protection guarantees as enshrined in Article 8 EUCFR, and further elaborated in general and sectoral instruments, should be considered as providing the modes for achieving respect for private life. In this sense, data protection will continue to maintain an important role *in light* of the right to private life. A systematic analysis of the analytical pattern followed by the Luxembourg Court when faced with cases involving the interaction between the two rights confirms this approach, which is further in line with the ECtHR’s case law. In a series of judgments, the importance of privacy is highlighted as the point of reference even in cases where the referring Court has asked for the interpretation of rules solely in terms of the right to the protection of personal data.

The systematic collection and storage of personal data has been repeatedly considered by the ECtHR as challenging the right to private life, irrespective of whether the data are further used or the collection took place in an intrusive manner (*Amann v Switzerland, Rotaru v Romania, Kopp v Switzerland*). Retention of biometric identifiers has also been regarded as ‘not unconsequential, irrelevant or neutral’ (*S and Marper* and *Schwarz*). These findings are directly applicable to immigration databases, the function of which is based on the registration of personal data, alphanumeric and biometric, in large-scale information systems. Furthermore, transmission of data to other authorities, and the subsequent use by them, enlarging the group of individuals with knowledge of the personal data amounts to a separate interference (*Weber and Saravia v Germany*).

The constitutive elements of privacy protection in relation to the processing of personal data in a systematic manner can be discerned by scrutinising the relevant jurisprudence of the Strasbourg and Luxembourg Courts, which over the past years have
developed a form of dialogue and cross-fertilisation.\textsuperscript{455} According to the ECtHR, to comply with the foreseeability requirement, the following conditions must be laid down in the applicable law:

a) In cases involving secret controls conducted by the police in sectors affecting national security, it is sufficient for the law to adequately indicate the circumstances in which, and the conditions on which, public authorities are authorised to interfere with privacy (\textit{Leander v Sweden});

b) The categories of data recorded must be defined (\textit{Rotaru v Romania});

c) The categories of people whose data are collected and stored must be specified (\textit{Rotaru v Romania, Amann v Switzerland});

d) The conditions and procedure under which collection, storage and further processing takes place must be set out (\textit{Rotaru v Switzerland, Amann v Switzerland});

e) The retention period must be specified taking into consideration the age of information stored (\textit{Rotaru v Romania, Leander v Sweden});

f) Rules regarding the persons authorised to access and consult the data must be provided, including the procedure that must followed for obtaining access (\textit{Rotaru v Romania});

g) The existence of supervision and judicial control mechanisms (\textit{Rotaru v Romania});

h) Reasonable suspicion against a person is substantiated when there are ‘factual indications’ for suspecting that person planning, committing, or having committed criminal acts or other acts (\textit{Zakharov v Russia}); and

i) The types of offences triggering an interference must be defined (\textit{Kennedy v UK}).

In order to establish whether an interference with – or in EU terms, a limitation to – the right to private life is proportionate to the aim pursued, both Courts have searched for a balance between States’ demands and the requirements of the protection of the individual’s fundamental rights. The scope of the margin of appreciation enjoyed by the EU legislator depends on a series of factors: the nature and seriousness of the interests at stake, the nature and gravity of the interference, and the objective pursued (\textit{Z v Finland, Peck v UK, S and Marper, Digital Rights Ireland}).

As for substantial standards for compliance with the right to private life, the ECtHR and CJEU have based their conclusions on the following considerations:

\textsuperscript{455} The ECtHR has made references to \textit{Digital Rights Ireland} in \textit{Zakharov v Russia} (n\textsuperscript{272} ¶147 and \textit{Szabó and Vissy v Hungary}, Appl no 37138/14 (12.01.2016) ¶23.
a) Retention of biometrics of persons who have not been suspected of a criminal offence may lead to discrimination and stigmatisation and may further disregard the presumption of innocence (S and Marper v UK);

b) The age of persons whose data are stored must be taken into account (S and Marper v UK);

c) A distinction between serious and lesser offences, or more generally a definition of criminal offences, justifying access is crucial (S and Marper v UK, Digital Rights Ireland);

d) The right of rectification of data must be ensured (S and Marper v UK);

e) Independent review must be safeguarded on the basis of pre-defined criteria (S and Marper v UK);

f) Retention periods must be limited on the basis of the data’s potential usefulness and should remain as short as possible (S and Marper v UK, Digital Rights Ireland);

g) Persons required to provide their fingerprint data in order to obtain a passport cannot be deemed to have consented to the processing of their fingerprints (Schwarz);

h) With regard to biometric identification, the impact on the individual is central both in terms of the possibility of a false match and as regards to the registration of fingerprint data per se (Schwarz);

i) Storage of data comprising of two fingerprints in a medium which remain with their owner is proportionate (Schwarz);

j) Generalised surveillance by mandating the collection, retention and storage of everyday personal data frustrates the relationship between the individual and the State by placing affected individuals under a constant state of suspicion (Digital Rights Ireland);

k) Indiscriminate collection of personal data without any differentiation, limitation or exception is unlawful. Data retention must be confined to situations which pose a threat to public security by restricting the measure to a time period, to a geographical zone, or to groups of persons likely to be involved in a serious crime, or more broadly to persons whose communications may contribute to law enforcement (Digital Rights Ireland, Schrems);

l) Ex post access and further processing should be subject to further requirements; it must be restricted to what is strictly necessary and must respect procedural and substantive conditions. Access should be limited to the purposes of preventing, detecting, and prosecuting well-defined serious offences. Finally,
requests for access should be conditional upon prior review by a court or an independent administrative body (Digital Rights Ireland); and

m) Data security throughout the retention period must be ensured (Digital Rights Ireland).

The aforementioned standards are applicable to the collection of personal data for immigration and border control purposes as guidelines for navigation and sources of inspiration. They become even more relevant in cases where immigration control mechanisms are used for criminal law purposes. Having in mind this toolkit, the next Chapters each examine the establishment and operation of EU immigration databases – both operational and on paper – starting with the oldest one, the Schengen Information System (SIS).
CHAPTER 2. The ‘Success Story’ of the Schengen Information System (SIS): A Reporting System Transformed into an Investigatory Tool

It has been clear from the earliest conception of SIS II that this system should be a flexible tool, that will be able to adapt to changed circumstances and fulfil, within a reasonable time and without major additional costs and efforts, user requests made during its lifecycle.456

1. Introduction

The SIS – and its newest configuration, the SIS II – is perhaps the best-known multinational database, which became operational in 1995 as a ‘flanking’ measure for the abolition of internal borders in the Schengen area. Its overarching purpose is to ensure a high level of security across the participating States and facilitate the movement of persons. To this end, national authorities are enabled to register so-called ‘alerts’ in relation to specific categories of persons and objects that are essentially requests by the State that issued the alert to the other Schengen countries to take a certain action.457 By default, the database is designed to perform as a hybrid instrument; on the one hand, as a tool for police and judicial cooperation in criminal matters, and on the other hand, as an instrument for immigration and border control.458 Under its latter function, national competent authorities are required to store alerts that comprise a series of personal data, including biometrics, on undesirable third-country nationals who must be refused entry or stay in the Schengen territory. The sui generis nature of the system is exemplified by the existence of three separate instruments governing the operation of the SIS II: a Regulation which focuses on third-country nationals to be refused entry into the Schengen area,459 another Regulation which refers to the use of

the database by the national authorities responsible for issuing vehicle registration certificates, and a Council Decision falling within the scope of police and judicial cooperation.

In this Chapter, I examine the immigration branch of the database in light of the right to private life. Firstly, I place the SIS within its historical framework, by providing a brief overview of Schengen cooperation. Secondly, I outline the key characteristics of the first generation SIS by emphasising on the registration of alerts on unwanted third-country nationals. Then, I focus on the setting up of the SIS II, including the current functionalities of the database and possible changes in the future. Finally, the fifth section is devoted to a legal analysis of the privacy concerns raised by the establishment, operation and reconfiguration of the system.

2. Schengen cooperation in a nutshell

On 14 June 1985, five EC Member States – Belgium, Luxembourg, Germany, France and the Netherlands – signed in Schengen an intergovernmental agreement providing for the gradual abolition of internal border checks among its signatories. This agreement was followed by an Implementing Convention (CISA), which was signed on 19 June 1990 and became effective on 26 March 1995, by which time Italy, Portugal, Spain, Greece and Austria had joined the Schengen zone. Its territorial scope progressively expanded, as most of the remaining Member States signed up to the Schengen Convention alongside the Nordic countries.

---

464 Italy (1990), Portugal and Spain (1991), Greece (1991) and Austria (1995).
465 Denmark, Finland and Sweden joined in 1996 along with Iceland and Norway as associate members. For further information on the development of Schengen see among others Monica den Boer (ed), Schengen, Judicial Cooperation and Policy Coordination (European Institute of Public Administration 1997); The Implementation of Schengen: First the Widening, Now the Deepening (European Institute of Public Administration 1997). On the relationship between Schengen and the Nordic countries see Kim Kjaer, ‘How Many Borders in the EU?’ in Kees Groenendijk, Elspeth Guild and Paul Minderhoud (eds), In Search of Europe’s Borders (Kluwer 2003).
The main objective of the Schengen experiment was to abolish internal controls between the signatory countries in lieu of a common external frontier. The underlying principle was dual purpose: to facilitate the free movement of persons and goods within the Schengen area, and to guarantee a high level of security. The logic behind the Schengen rules was that once a person has been allowed to cross the common external border, they might automatically circulate within the Schengen area, without being subjected again to checks at the border of a participating country. However, this free circulation of persons implies that irregular migrants and criminals will also move freely. In fear of this scenario, a series of ‘compensatory’ measures were deemed necessary to counterbalance the elimination of internal border controls. In this context, the CISA laid down extensive measures to the abolition of internal controls and the free movement of persons within the Schengen territory, in particular rules on: the enhancement of external border controls; harmonisation of visa policies and regulation of movement of third-country nationals; irregular immigration; allocation of responsibility for asylum requests; mutual assistance in criminal matters and strengthened police cooperation on the basis of information exchange through a multinational database to be used by immigration, border control, police and judicial authorities. That database was the SIS.

In May 1999, the Schengen rules were integrated in the secondary Community and Union law by means of a Protocol attached to the Amsterdam Treaty. The Schengen acquis extended fully to all the fifteen States that were then members of the EU, except for the UK, Ireland and Denmark, which signed separate Protocols acquiring special privileges. In May 2004, ten States acceded into the EU, among which only Cyprus has not yet become a member of the Schengen zone. The newest members of the EU family, Bulgaria, Romania and Croatia, have signed accession agreements but the rules are yet to be implemented. In addition, Norway, Iceland, Switzerland and

---

466 CISA, art 187.
467 Dumortier (n457) 93.
468 Kabera Karanja (n29) 51.
469 CISA, arts 1-25.
470 ibid arts 26-7.
471 ibid arts 28-38.
472 ibid arts 39-91.
473 ibid arts 92-119.
Liechtenstein form part of the Schengen area without holding an EU membership, as Schengen Associate States. \(^{476}\) Hence, the Schengen area currently comprises of 26 participating countries.

3. The Schengen Information System (SIS)

3.1 Step one: The establishment of the SIS

3.1.1 Introduction to the SIS

The SIS has been eloquently characterised as the ‘heart of the compensatory measures designed to play a key role in minimizing the deficits of the abolition of internal border controls’. \(^{477}\) It was set up under the CISA \(^{478}\) and came into operation on 26 March 1995 \(^{479}\) as a support tool for national competent authorities. According to Article 93 CISA, its objective was twofold: a) to maintain public order and security, including State security; and b) to enable the Contracting parties to automatically search the information on persons and objects registered therein for the purposes of border control and police investigations, control and other searches. Therefore, on the one hand, it could be used by national police, customs and border control authorities when performing checks on persons at external borders or within Schengen states, and, on the other hand, it could assist immigration officers when administering third-country nationals, particularly in relation to issuing visas and residence permits. \(^{480}\) By its very nature, the SIS thus served as both an immigration and a criminal law instrument.

The SIS held data categorised in the form of ‘alerts’ on various categories of persons and objects, including information on third-country nationals to be refused

---


\(^{478}\) CISA, art 92.

\(^{479}\) The original conceptualisation of the database was a German initiative of late 1985. The setting up of the database was agreed upon in September 1987. Brouwer (n17) 49.

\(^{480}\) CISA, art 92.
entry into the Schengen area (Article 96). National competent authorities could search
the system through an automatic, direct query procedure to check whether an individual
or an object had been registered into the SIS and what action needed to be taken in
accordance with the alert.\textsuperscript{481} In effect, the database had limited capacities as it operated
on a hit/no hit basis in order to allow for speedy results.

Each SIS alert was composed of a specific set of alphanumeric data; the name and
surname of the person concerned, any specific objective physical characteristics not
subject to change, the place and date of birth, sex, nationality, information on whether
persons concerned are armed, violent or have escaped, the reason for the alert, the
action to be taken and, in case of persons wanted for extradition purposes, the criminal
offence they had committed.\textsuperscript{482} In practice, the possibility of entering any specific
objective physical characteristics left wide discretion to the registering authorities to
include information that could reveal racial origin (for instance, the colour of the person
concerned) signifying that sensitive information could be stored.\textsuperscript{483} Access to data was
reserved for relevant policing, border control, immigration or customs authorities, but
officials could conduct searches only in relation to their tasks.\textsuperscript{484} The decision on
whether a national authority had access to a certain type of data was in principle a
national prerogative.\textsuperscript{485} Nevertheless, pursuant to Article 101(4), the participating States
had to notify on the appointed authorities on a yearly basis.

The operation of the SIS as an information exchange tool was enabled by its
architecture, comprising a national system (N.SIS) in each participating State, and a
central database (C.SIS) located in France, complemented by a back-up system in
Austria.\textsuperscript{486} The SIS was supplemented by an auxiliary system named SIRENE, which
provided the infrastructure for exchanging additional information to that held in the SIS,
as well as facilitating the exchange of police information taking place outside the SIS.\textsuperscript{487}
Every participating State set up a SIRENE bureau responsible for the smooth operation
of its N.SIS.\textsuperscript{488} SIRENE was intended as the depository of supplementary information in

\textsuperscript{481} For example, an alert on person wanted for extradition purposes would require the national
authorities to arrest them. An alert on a third-country national would signify that this person should be
refused entry to the Schengen territory.
\textsuperscript{482} CISA, art 94(1).
\textsuperscript{483} Kabera Karanja (n29) 189.
\textsuperscript{484} CISA, art 101.
\textsuperscript{485} For the procedure of entering an alert see Kabera Karanja (n29) 184-5.
\textsuperscript{486} The management of the system was delegated by the Commission to France and Austria.
\textsuperscript{487} The legal basis of the SIRENE was criticised as confusing and contentious as CISA did not include
any information. This perplex legal framework was resolved with the adoption of Council Decision
2005/211/JHA and Regulation 872/2004, which amended art 92 CISA. See below, Section 3.2.2 On
functioning of SIRENE see Kabera Karanja (n29) 202-208.
\textsuperscript{488} CISA, art 108.
relation to all national entries, at the disposal of other participating States if so required.\textsuperscript{489} In that sense, the SIS practically served as an index to the SIRENE system.\textsuperscript{490}

A particularly controversial issue concerned the allocation of a legal basis for every instrument of the Schengen \textit{acquis} in view of its incorporation into the EU legal order. For most of the instruments this operation ran smooth, but not for the SIS.\textsuperscript{491} Despite its dual function, the SIS remained almost entirely a ‘third pillar’ measure,\textsuperscript{492} because many Member States considered as ‘anathema’\textsuperscript{493} the possibility to allocate the database to both a first and a third pillar legal basis. However, the Amsterdam Treaty required that any new measures building upon the \textit{acquis} had to be adopted on the correct legal bases.\textsuperscript{494} Therefore, despite the original failure to agree on the legal base for the SIS provisions, measures adopted subsequently were allocated to the correct legal basis.\textsuperscript{495}

### 3.1.2 Alerts on third-country nationals: Keeping away the ‘unwanted’

The original concept regarding the SIS was to establish a mechanism that would be used solely for security and police-related purposes.\textsuperscript{496} The idea of exchanging information on ‘inadmissible aliens’ through the SIS came from the existing cooperation scheme in the Benelux countries designed for sharing information on individuals who had to be refused entry at their external borders.\textsuperscript{497} As early as in April 1988, the Dutch delegation put forward a proposal for storing information on certain categories of third-country nationals that would not be admitted entry.\textsuperscript{498} The proposal involved persons against whom a formal residence ban had been issued and persons

---

\textsuperscript{489} The SIRENE information may be extensive and non-standardised. Kabera Karanja (n29) 207.

\textsuperscript{490} Broeders (n25) 80.

\textsuperscript{491} Council Decision 1999/435 of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis \cite[1999][]{19991761}; Council Decision 1999/436 of 20 May 1999 determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the Schengen acquis \cite[1999][]{199917617}. For the publication of the whole Schengen \textit{acquis}, except for the confidential sections \cite[2000][]{1999L391}.

\textsuperscript{492} Steve Peers, ‘Key Legislative Developments on Migration in the European Union: SIS II’ \cite[2008][]{200777} 10 \textit{European Journal of Migration and Law} 77, 79.

\textsuperscript{493} Kuijper (n474) 349.

\textsuperscript{494} Niels Bracke, ‘Flexibility, Justice Cooperation and the Treaty of Amsterdam’ in Clotilde Marinho (ed), \textit{Asylum, Immigration and Schengen Post Amsterdam} (EIPA 2001) 59.

\textsuperscript{495} Tzanou (n31) 149.

\textsuperscript{496} Brouwer (n17) 59-60.

\textsuperscript{497} ibid 47.

\textsuperscript{498} ibid 60.
who were reported as inadmissible. An additional suggestion concerned the inclusion of alerts on persons to whom no visa should be issued without prior approval by the national visa agency, and alerts on persons whose asylum application had failed.

The final wording of Article 96 CISA stipulated three grounds for registering alerts on third-country nationals into the system, broadly relating to third-country nationals either linked to criminal activity, thus threatening public policy, public security or national security, or in breach of national immigration laws:

‘2. Decisions may be based on a threat to public policy or public security or to national security which the presence of an alien in national territory may pose.

This situation may arise in particular in the case of:
(a) an alien who has been convicted of an offence carrying a penalty involving deprivation of liberty of at least one year;
(b) an alien in respect of whom there are serious grounds for believing that he has committed serious criminal offences, including those referred to in Article 71, or in respect of whom there is clear evidence of an intention to commit such offences in the territory of a Contracting Party.

3. Decisions may also be based on the fact that the alien has been subject to measures involving deportation, refusal of entry or removal which have not been rescinded or suspended, including or accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of aliens.’

The consequence of an alert was a form of mutual recognition of another Member State’s decision in this field, since, in principle, the person concerned would be precluded from entering the Schengen area. Similarly, in case a third-country national registered in the system applied for a short-stay visa, national authorities would have to reject the application.

The registration of an alert was based on national decisions by administrative authorities or the judiciary. Strikingly, no harmonised criteria for issuing national decisions were specified. As Guild has astutely observed, there was ‘extraordinary

---

499 Emphasis added.
501 CISA, art 15. According to art 18, the SIS would be consulted before the issuance of a long-stay visa as well.
502 Ibid art 92(1).
flexibility of the criteria on the basis of which somebody may be registered in the SIS, and [...] very wide degree of discretion which is left to a particular Member State official to insert someone’s information into the SIS.\(^{503}\) The mere wording of Article 96 entailed that if an individual matched the prescribed criteria, this would be enough for being deemed as a threat to public order, public security or irregular migration.\(^{504}\) Furthermore, Member States did not have to further reason the insertion of an alert, but pursuant to Article 94, the case had to be ‘important enough’ to be reported in the system. Apparently, Member States were stuck in between two competing driving forces: to prevent arbitrary implementation as regards to inadmissible third-country nationals, whilst ensuring enough discretionary power to national authorities.\(^{505}\) As a result, the abstract concepts of ‘public policy’ and ‘public security’ were left for interpretation at the domestic level.\(^{506}\) Nevertheless, as Brouwer has observed, the assumption that the criteria could not have been better aligned was more of a ‘political rather than a legal reality’.\(^{507}\) In a series of judgments pronounced by the ECJ relating to the free movement of EU nationals and privileged non-EU nationals, the concept of ‘public order and security’ had been elaborated, which could have applied to a wider group of non-EU nationals.\(^{508}\)

The legislation translated in high discrepancies regarding the interpretation of the grounds at the national level, which persisted years after the SIS had become operational. An important issue in this respect has been the fact that decisions on registering alerts could be taken ‘at a relatively low level’.\(^{509}\) As a result, it has been reported\(^{510}\) that German authorities inserted alerts \textit{en masse} on all failed asylum seekers, whereas Italian officials entered information on all irregular migrants without

---


\(^{504}\) Brouwer (n17) 62.

\(^{505}\) ibid.


\(^{507}\) Brouwer (n17) 62.

\(^{508}\) ibid; Case 30/77 Bouchereau [1977] ECR 01999; Joined Cases 115/81 and 116/81 Rezgua Adoui v Belgian State and City of Liège (115/81) and Dominique Cormuaille v Belgian State (116/81) [1982] ECR 01665.


These Member States were far more active in using the system, accounting for roughly 77% of all the alerts under Article 96 CISA, raising serious concerns regarding the lawfulness of the immigration part of the system. Furthermore, other States automatically inserted alerts to the SIS whenever a return decision was issued, or following a decision to refuse entry. From the perspective of the individual, this lack of uniform criteria signified that third-country nationals could receive fundamentally different treatment and assessment depending on whether they were ‘fortunate’ (or unfortunate) to fall within the competence of specific Member States or officials. As for the magnitude of the problem, the SIS was mainly preoccupied – and, as will be seen below, still is – with keeping undesirable third-country nationals outside the Schengen territory. Additionally, this lack of guidance was further evident in routine renewals of alerts after the initial three-year retention period had expired.

3.2 Step two: The reinvigoration of the SIS in the aftermath of 9/11

3.2.1 Thinking ‘outside of the box’ - Far-reaching suggestions by Member States

The terrorist events of 9/11, coupled with the Madrid bombings of 2004, had a profound impact on the operation of the SIS. In the Extraordinary Council Meeting that took place immediately after the 2001 attacks, the Council announced that it would examine the possibility of allowing other public services to consult the system and

---

511 Kabera Kananja and Brouwer mention the Forabosco case brought before the French Conseil d’État, where the Court criticised the German practice to register alerts on failed asylum applicants in the SIS. Conseil d’État, M et Mme Forabosco (no 190384, 09.06.1999). See Kabera Karanja (n29) 215; Brouwer (n17) 370-1.

512 Kabera Karanja (n29) 214.


515 For an overview of the statistics until 2006 see Brouwer (n17) 65-70. For the latest statistics before migration to the SIS II see Council, Document 7389/13 (13.03.2013).

called for more systematic input into the SIS of alerts including Article 96 CISA.\textsuperscript{517} In the following months, different Member States put forward numerous ideas concerning the expansion of the SIS. The Germans suggested a possible interconnection of data allowing Europol, National Prosecutors’ Offices and immigration and asylum authorities access to the SIS.\textsuperscript{518} The Belgians proposed an extension of Article 96 CISA with a view to checking whether a third-country national to whom a visa was issued, and whose visa had expired, have actually left the Schengen area.\textsuperscript{519} A UK proposal involved possible access to the SIS by internal security and intelligence services.\textsuperscript{520} Though no formal decision was taken, it has been submitted that, based on an informal decision at working party level, SIS access by security and intelligence services was implemented at national level without a formal legal basis.\textsuperscript{521} An important proposal related to the registration of persons included in the UN terrorist list established by the Sanctions Committee on Afghanistan, based on UN Security Council Resolution 1390/2002. Eventually, no official decision was taken, but pursuant to an informal agreement between the Schengen States, the German authorities agreed to enter the listed persons into the SIS on behalf of all States.\textsuperscript{522}

3.2.2 The Spanish initiative

Of the proposed ideas, two pieces of legislation were eventually adopted at Spain’s initiative.\textsuperscript{523} Regulation 871/2004\textsuperscript{524} and Council Decision 2005/211/JHA\textsuperscript{525} aimed to

\textsuperscript{517} Council, Document 12019/01 (Presse 327, 20.09.2001) pts 13 and 27.
\textsuperscript{518} Council, Document SN 4038/01 (27.09.2001).
\textsuperscript{519} Council, Document 12813/01 (15.10.2001); This proposal was transferred in what later became the VIS and the EES. See Chapters 3 and 5.
\textsuperscript{520} Council, Document 13530/01 (29.10.2001). See Council, Documents 13269/01 (31.10.2001); 10127/02 (21.06.2002).
\textsuperscript{521} Ben Hayes, ‘From the Schengen Information System to the SIS II and the Visa Information System (VIS): The Proposals Explained’ (Statewatch 2004) 9.
\textsuperscript{522} Council, Document 9182/03 (12.05.2003). See Council, Document 7783/06 (07.04.2006).
improve the SIS capabilities as a response to the fight against terrorism. The measures adopted involved:

a) Access by Europol and Eurojust to certain categories of data of the criminal law branch;\(^{526}\)
b) Access to SIS data, including the immigration branch, by national judicial authorities, including public prosecutors;\(^{527}\) and
c) Access to information held in the SIS on stolen, misappropriated or lost identity documents by authorities responsible for issuing or examining visa applications or for issuing residence permits.\(^{528}\)

Furthermore, the Regulation mandated the recording of transmissions of personal data\(^{529}\) and reference was made to the SIRENE offices providing a legal basis for their operation.\(^{530}\)

The idea of opening up the SIS to Europol and Eurojust had been advocated by Germany already since 1998.\(^{531}\) In the wake of the 9/11 events, the discussions about granting access to these agencies gained a fresh impetus and indeed a year later Member States reached agreement in this respect.\(^{532}\) At that time, no distinction was made between the different types of alerts, and nor did the Spanish proposal make such a distinction. During the negotiations for the adoption of the Regulation, however, the issue proved particularly controversial.\(^{533}\) Eventually no agreement was reached and access to Europol and Eurojust was reserved for specific categories of alerts inserted in the SIS, but not relating to its immigration branch.

Although access to Article 96 data by Europol and Eurojust was not granted, Regulation 872/2004 includes an amendment to Article (1)(b) CISA concerning the authorities having direct access to the SIS. Under the new regime, direct consultation was made possible for national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks.\(^{534}\) Notably some Member States already allowed access to the SIS to their public prosecutors based on the previous wording of Article 101(1)(b), according to which authorities that could have access to the SIS are those ‘responsible for police and customs checks […] and the coordination of such

\(^{526}\) ibid art 1(9).
\(^{527}\) Regulation 871/2004, art 1(3).
\(^{528}\) ibid art 1(6).
\(^{529}\) ibid art 1(2).
\(^{530}\) Ibid art 1(1).
\(^{531}\) Council, Documents 10629/99 (20.08.1999); 11538/2000 (20.09.2000).
\(^{533}\) See Council, Documents 9408/4/02 (26.11.2002); 11653/02 (02.09.2002).
\(^{534}\) Regulation 871/2004, art 1(3).
Therefore, the Spanish proposal did not contain a special paragraph on granting access to the judicial authorities; it rather proposed a mere addition to the accessibility by police and customs authorities ‘and the judicial supervision thereof’. 536 As it has been rightly pointed out, the mere possibility for national judicial authorities to access the database signaled a shift in the use of third-country nationals’ data from purely immigration purposes to criminal law objectives. 537 This means that the security continuum that was partly avoided with the resistance in granting access to Article 96 data to Europol and Eurojust was, after all, established. 538 In addition, as Hayes has stressed, the national judicial authorities have developed relationships with Europol, and especially Eurojust, meaning that it is possible that the direct prohibition as prescribed in the Regulation could be by-passed. 539

4. The second generation Schengen Information System (SIS II)

4.1 Step three: The set up of the SIS II

4.1.1 The long and winding road to the SIS II

The idea of the transition from the SIS to the SIS II dates back to 1996 when the then Schengen States reflected on technical and functional improvements of the database, particularly in view the forthcoming integration into the SIS of the Nordic countries. In December 1996, when Denmark, Sweden and Finland signed their respective agreements on joining the Schengen zone, it was already established that a new database would have to be developed. The system would not only be able to accommodate newcomers in the Schengen family, but would include new functionalities. 540

---

535 Emphasis added.
536 Spanish Initiative (n523) art 1(1).
538 Ibid.
539 Hayes, ‘From the Schengen Information System’ (n521) 86.
540 This decision was not published but is referred to in the decision of the Schengen Executive Committee of 25 April 1997 in which Portugal was mandated to start a preliminary study for SIS II. (SCH/Com-ex (97) 2 rev. 2) published in [2000] OJ L239/1. See House of Lords (n503) 12.
The need for establishing the SIS II became pressing, as from May 2004 ten more countries would accede the EU and the system could technically accommodate no more than 18 countries. Therefore, Regulation 2001/2424\textsuperscript{541} and Decision 2001/886\textsuperscript{542} were adopted providing the legal basis for the setting up of the new system. The SIS II was planned to go live in October 2007, parallel to the date when the new Member States were scheduled to join the Schengen area. However, numerous legal and technical complications were encountered resulting in significant delays.\textsuperscript{543} An interim solution called ‘SISone4all’ was implemented so as to enable the new Member States to join the system as soon as possible.\textsuperscript{544} In the following years, the SIS legislative framework grew as a series of intermediary instruments were adopted in view of migrating from the SIS (renamed to SIS 1+) to the SIS II.\textsuperscript{545} and due to consecutive postponements of the deadline for that transition.\textsuperscript{546} Eventually, on 25 February 2013, the Council adopted two Decisions\textsuperscript{547} concerning the date of application of the SIS II instruments, and the SIS II finally launched on 9 April 2013.

\textsuperscript{543} For an overview see Joanna Parkin, ‘The Difficult Road to the Schengen Information System II - The Legacy of Laboratories and the Cost for Fundamental Rights and the Rule of Law’ (CEPS 2011).
4.1.2 Introduction to the SIS II

Although officially the pushing factor for developing the SIS II was to improve the capacity of the system in order to accommodate a larger group of States, the momentum was used to introduce new functionalities and technical features. Following the events of 9/11, several proposals made their way into draft texts on SIS II. The underlying rationale was to make the SIS II ‘a flexible tool’, that could be used ‘for other purposes than those originally foreseen, and especially for police information purposes in a broad sense’. In June 2002, the Ecofin Council agreed to enable the system to process biometrics and additional categories of information, interlink different types of alerts and conduct searches on the basis of incomplete data. With the exception of the latter element, these functions feature in the final text.

On 31 May 2005, the Commission presented proposals for three legislative instruments governing the SIS II: a (former first pillar) Regulation concerning the immigration aspects of the system to be adopted under Title IV of the EC Treaty; another Regulation (former first pillar) concerning access to the system by vehicle registration authorities to be based on Title V (Transport) of the EC Treaty; and a (former third pillar) Council Decision regarding the use of the system for policing and criminal law purposes to be based on Title IV of the EU Treaty. Separate proposals were necessary due to the different legal bases and the different decision-making processes concerned. However, it is highlighted that this arrangement ‘did not affect the principle that SIS II constitutes one single information system that should operate as such’. Strikingly the main points on the new features were almost decided within the Council before any official scrutiny by the Parliament, the involvement of which was evident only after the new legislation was proposed. It has been pointed out that in reality the Parliament was well aware of what the Council desired, and in any case

---

548 For a list of proposals on what elements to add see Brouwer (n17) 87.
549 For example see Council, Document SN 12463/02 (21/22.06.2002) pt 30.
550 Council, Document 9808/03 (n456) 6.
551 Council, Document 5968/02 (05.02.2002) 2.
552 Council, Document 10089/02 (Presse 181, 20.06.2002). It was pointed out that these features would ensure ‘greater effectiveness in combating terrorism’.
556 Peers, ‘Key Legislative Developments’ (n492) 81.
557 SIS II regulation, recital 4; SIS II Decision, recital 4.
558 Parkin (n543) 23-4.
during the negotiations the final text was subject to a series of amendments.\footnote{Informal discussion with an MEP (Brussels, December 2014).} Key in this context was that the MEP Rapporteur Carlos Coelho insisted that all three measures should be discussed as a package.

The two Regulations were adopted on 20 December 2006,\footnote{See n459-60.} whereas the Decision was adopted on 12 June 2007.\footnote{See n461.} They came into effect on 9 April 2013 when the SIS II became operational. The categories of alerts that can be inserted into the system are formulated as follows:

a) Third-country nationals to be refused entry or stay (Article 20, Regulation 1987/2006);

b) Persons wanted for arrest or surrender purposes (Article 26, Council Decision 2007/533);

c) Missing persons (Article 30, Council Decision 2007/533);

d) Persons sought to assist with a judicial procedure (Article 34, Council Decision 2007/533);

e) Persons and objects for discreet checks or specific checks (Article 36, Council Decision 2007/533); and

f) Objects sought for the purpose of seizure or use as evidence in criminal proceedings (Article 38, Council Decision 2007/533).

According to the latest statistics concerning the year 2015, the alerts on undesirable third-country nationals still dominate the content of the database. Of the total 793,318 alerts on persons included in the system, 492,655 have been inserted for immigration purposes, amounting to 62.1% of the total number of alerts issued.\footnote{eu-LISA, ‘SIS II – 2015 Statistics’ (2016) 10-1. In comparison to previous statistics there is a marked decreased in the rates.} Of all the 156,447 hits produced in 2015, 30,501 involved third-country nationals.\footnote{ibid 12.}

The architecture has remained relatively the same: a central system (the Central SIS II), comprising of a technical support system (referred to as CS-SIS) and uniform national interfaces (NI-SIS) on the one hand, and national sections (N.SIS II) on the other hand. The only difference is that national interfaces will not hold the data, but Member States may choose to maintain, as part of the N.SIS II, a ‘national copy’ of the database.\footnote{SIS II Regulation, art 4(1).} SIRENE remains the forum for any supplementary information exchange and coordination of activities connected to SIS II alerts.\footnote{For the SIRENE-related legislation see Commission Decision 2008/333/EC of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) [2008] OJ L123/1; Commission Decision 2008/334/JHA of 4 March 2008} Currently, the territorial...
The scope of the SIS II is as follows: EU Member States that participate in Schengen cooperation and associated Schengen States operate the SIS. The UK, Bulgaria and Romania currently use the SIS for the purpose of law enforcement cooperation only. The use of the SIS in the external border control context will commence as soon as the decision for lifting internal border checks becomes effective. Furthermore, Ireland, Cyprus and Croatia are currently carrying out preparatory activities pending integration into the SIS.

4.1.3 Overview of the SIS II Regulation

a) Scope and purpose

Regulation 1987/2006 constitutes the legal instrument for governing the immigration and border control aspects of the SIS II. According to its Article 1(2), the purpose of the database is:

‘to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the Treaty relating to the movement of persons in their territories, using information communicated via this system’.

Two objectives can be identified in this regard: a more general one concerning the ‘maintenance of public security and public policy’ and a more specific one regarding the exchange of information for the purposes of controls on persons and objects. Both purposes, however, are understood under the overarching aim of ensuring a high level of security within the EU.

566 Council Decision of 14 December 2010 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [2010] OJ L333/38.

567 Ireland shall be able to operate the SIS solely for law enforcement purposes.

568 Compare with art 1(2) of the Commission proposal for a SIS II Regulation which stated that ‘(t)he SIS II would contribute to maintaining a high level of security’.
The emphatic reference to the notion of ‘security’ cannot go unnoticed. It signals a reinforced focus on security in EU policy in relation to the use of the SIS II,\(^{569}\) which is particularly problematic in relation to the immigration branch of the system. Considering that the predominant use of the system *de facto* involved the refusal of entry of unwelcome third-country nationals, the revised framework should have taken stock of this fact.

Furthermore, in comparison to Article 93(1) CISA, the general scope of the SIS II is framed in even broader terms than in relation to the SIS. The vague wording seems to suggest that the system is no longer restricted to police and judicial cooperation by assisting in controlling persons and objects, but may be used as a tool to support police and judicial cooperation in a more general manner.\(^{570}\) Expanding the purpose of the SIS through vague terminology leaves wide discretionary power for interpretation by the Member States,\(^{571}\) and triggers uncertainty concerning the possibilities of the use of the SIS II for the exchange of information between the police and judicial authorities in practice. These concerns are not merely theoretical; as highlighted above, the Council already since 2002 took note of the dynamic nature of the SIS that could extend beyond its traditional role as a compensatory instrument for the abolition of internal border control. As it has been pointed out, understanding the SIS II as a ‘flexible system based on new technology’ implies a gradual but steady transformation of the database from a reporting tool to a far more advanced, investigative instrument, which may serve various purposes.\(^{572}\) In addition, these concerns are further heightened taking into consideration the lack of impact assessment or an explanatory memorandum attached to proposals.\(^{573}\)

**b) Categories of registered data**

Under the CISA rules the old database contained only a relatively limited set of elements per alert. The SIS II Regulation requires additional alphanumeric data to be recorded into the system, namely information on multiple nationalities, the authority

---

\(^{569}\) Brouwer (n17) 93.


\(^{571}\) ibid.

\(^{572}\) This transformation was observed by the Commission already in 2001. Commission, ‘Development of the Schengen Information System II’ (Communication) COM(2001) 720 final.

\(^{573}\) Given that these were recast proposals on an existing scheme, in principle it was not obligatory for either these documents. However, given the substantial changes inserted, the conduct of an Impact Assessment was necessary. The EDPS notes in this respect: ‘It is in many respects difficult to know what the intention behind the texts is’. EDPS, ‘Opinion on SIS II proposals’ (n352) 39.
issuing the alert, a reference to the decision giving rise to the alert and links to other alerts issued into the system.\textsuperscript{574} Importantly, the system records biometric identifiers, in particular photographs and fingerprints.\textsuperscript{575} As mentioned earlier, the Council agreement, in principle, on the inclusion of biometrics was reached in June 2002, however the idea was first discussed in 2000 alongside the possibility of adding DNA profiles into the system.\textsuperscript{576} The formal agreement was then reached at the Thessaloniki Council meeting of June 2003.\textsuperscript{577} This development should be seen in view of the function of Eurodac on the basis of fingerprints and the insertion of biometrics in the then negotiated VIS. In essence, the revised framework was a form of aligning the respective rules with the state of play of the remaining immigration databases. A key factor in this respect was the possibility to interlink the existing databases through a common AFIS, thus enabling checks on the basis of biometric data.\textsuperscript{578}

In this context, Article 22 prescribes that biometrics shall be processed in two phases:\textsuperscript{579} at first, biometric data are registered after a ‘special quality check’, the specifications of which were considered technical and were thus left for determination in ‘comitology’ procedure.\textsuperscript{580} As the EDPS rightly pointed out, the lack of specific requirements on how biometrics would be collected and stored is crucial, and such aspects should not be marginalised.\textsuperscript{581} In the first phase, photographs and fingerprints are used solely to ‘confirm the identity’ of an individual ‘who has been located’ after a ‘hit’ (one-to-one searches).\textsuperscript{582} When technically available, biometrics shall be used to ‘identify persons’. This new feature will apply following a report published by the Commission regarding the availability and readiness of the required technology after

\textsuperscript{574} SIS II Regulation, art 20(2). During the negotiations elements such as a single nationality of individuals, deletion of the reference on whether the person was armed, violent or had escaped and the inclusion of details regarding the specificities of the decision giving rise to the alert were also discussed. Council, Document 5709/06 (04.04.2006).
\textsuperscript{575} art 20(2)(e) and (f) SIS II Regulation.
\textsuperscript{576} Council, Document 12400/00 (27.10.2000).
\textsuperscript{577} Council, Document 11638/03 (n338).
\textsuperscript{579} For the vision of the Council in this respect see Council, Document 10125/04 (03.06.2004). The Council did not foresee the mandatory registration of photographs, but noted that in the second phase these would be used ‘for the purposes of identification of suspect persons’. For the negotiations see Council, Document 5709/3/06 (24.04.2006); Council, Document 8537/06 (20.04.2006).
\textsuperscript{580} Specifications on biometrics are included in the SIRENE manual (n565).
\textsuperscript{582} SIS II Regulation, art 22(b).
consultation with the EP, but without further vote within the EU institutions.\(^{583}\) Notably the EP Rapporteur opposed the use of biometrics for identification purposes, therefore, it was at the behest of the EP’s pressure that the wording of Article 22 was formulated accordingly, even though it had to compromise fundamentally on the initial objective of excluding identification searches in the future.\(^{584}\)

At the time of writing, the SIS II has not yet entered into its second phase. Border checks currently take place on the basis of alphanumeric data only, and fingerprints are used to confirm the identity of a person who has already been identified on the basis of his/her name.\(^{585}\) In an informal discussion with a Greek official using the database for operational purposes, it was mentioned that although national authorities could attach fingerprint data to an alert, these were visible to other authorities, but not available for consultation.\(^{586}\) The issue had stalled until March 2016, when the Commission released its report on the availability and readiness of the technology to identify a person on the basis of fingerprints held in the system, setting mid-2017 as the deadline for implementing the new functions.\(^{587}\) This new functionality will entail that in cases when the issuing Member State has access to the person in respect of whom the alert is issued, the ten fingerprints will be collected, attached to the alert and compared with the prints already stored in the system revealing possible links to other alerts.\(^{588}\) Latent fingerprints – that is incomplete fingerprints left at a crime scene – will also be used for consultation.

c) Substantive grounds for a listing in the SIS II

i) The ‘usual suspects’

Article 24 of the SIS II Regulation stipulating the criteria for entering alerts on unwanted third-country nationals largely replicates Article 96 CISA. The two main categories of reasons triggering the entry of an alert remain. Firstly, the registration of alerts in relation to third-country nationals who are considered to pose a threat to public

\(^{583}\) During the negotiations on the adoption of the legislative framework of SIS II, some Member States agreed on exchanging fingerprints and photographs, as supplementary information to the SIS information (SIREne Picture Transfer). See Brouwer (n17) 99.

\(^{584}\) Peers, ‘Key Legislative Developments’ (n492) 88.

\(^{585}\) Commission, ‘Stronger and smarter information systems for borders and security’ (Communication) COM(2016) 205 final, 7-8.

\(^{586}\) Interview with Greek official (Athens, August 2014).

\(^{587}\) Commission, ‘The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)’ (Report) COM(2016) 93 final.

\(^{588}\) ibid 7.
policy or public security, or to national security has become mandatory. This insertion shall arise, in particular, in cases where third-country nationals have been convicted in a Member State for a crime carrying a penalty of imprisonment of at least one year, or third-country nationals in respect of whom there are serious grounds for believing that they have committed a serious criminal offence, or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a participating country. The list of cases remains open-ended, thus Member States may register alerts on third-country nationals for other reasons based on public order or public security grounds. Under the second category of alerts, which may be entered in the system, all third-country nationals who have been subject to a measure involving expulsion, refusal of entry or removal, which has not been rescinded or suspended, including or accompanied by an entry ban, or where applicable, a prohibition of residence on the basis of a failure to comply with national immigration law.

The registration of an alert into the system is subject to two conditions: firstly, a decision to issue a national alert must be taken by the competent administrative authorities or courts in accordance with national law, and secondly, this national alert forms the basis for a SIS II alert. An important addition to Article 24(1) is that the national decision to issue an alert must be based on ‘an individual assessment’. The Commission proposal included this proviso as a separate sentence, but it was a requirement only in relation to the alerts inserted on criminal law and security grounds and not on immigration grounds. The importance of this rule cannot be overstressed. The EU legislator clarifies that, in principle, automaticity and registration of alerts en masse is not an option and that each case should be considered individually pursuant to the national criteria and the criteria set out in the SIS II Regulation. The requirement for ‘individual assessment’ must be read in combination with Article 21, which provides for a proportionality clause. The latter is a revised form of Article 94 CISA, which prescribed that Member States had to determine before issuing an alert that the case was important enough to warrant an entry of an alert in to the system. Under the new proportionality clause, the threshold is significantly higher; in addition to the importance assigned to each case, its adequacy and relevance must be taken into consideration as well. As Brouwer points out, there must be ‘a direct relationship’ between the cause for which a person is to be reported in the system and the added

589 In comparison with art 96(2) CISA, there has been a change in the wording. In specific, instead of a requirement for ‘clear evidence’ the threshold of proof is significantly lowered to ‘clear indications’. See Brouwer (n17) 96; Peers, EU Justice and Home Affairs Law (n475) 205.
590 SIS II Regulation, art 24(3).
591 See Council, Document 5709/6/06 (04.04.2006).
592 Commission, ‘Proposal for SIS II Regulation’ (n553) art 15.
593 Brouwer (n17) 95.
value of such registration to national authorities.\textsuperscript{594} Furthermore, the decision for issuing an alert is accompanied by a new right to an appeal.\textsuperscript{595}

The lack of harmonised rules on the recording of alerts was not satisfactorily addressed. The proposal attempted to streamline, at least to a certain extent, the grounds for registration. In particular, regarding the penalty framework imposed to an individual and could trigger an alert, the Commission referred to the offences listed in the Framework Decision on the EAW.\textsuperscript{596} Furthermore, in relation to third-country nationals subjected to a re-entry ban, there was a reference to the then negotiated Directive 2008/116/EC on the return of irregular migrants.\textsuperscript{597} Overall, Member States were less than enthusiastic with a possible harmonisation of the criteria for entering alerts. For instance, the German delegation noted that under their national law a number of offences listed in the Framework Decision were punishable by a custodial sentence of less than a year, or a pecuniary punishment, and as a result they may not be regarded as serious enough.\textsuperscript{598} Consequently, the then Austrian Presidency essentially redrafted the proposal and returned to the wording of Article 96 CISA.\textsuperscript{599} It was pointed out in this respect that the inability to reach agreement was due to the belief among the participating States that a radical departure from the existing rules could endanger the smooth transition from one system to the other, and would entail ‘a degradation of the effectiveness of the system compared to the existing SIS’.\textsuperscript{600} What was left in the final text was an explicit reference that the imposition of an entry ban could possibly trigger a SIS II alert and a sunset clause that, following the evaluation of the operation of the system, the Commission may propose further modifications to achieve ‘a greater level of harmonisation of the criteria for entering alerts’.\textsuperscript{601}

\textsuperscript{594}ibid.
\textsuperscript{595} SIS II Regulation, art 20(1). See Council, Document 5709/1/06 REV 1 ADD 1 (04.04.2006), 2.
\textsuperscript{598} Council, Document 5709/1/06 REV 1 ADD 7 (05.04.2006) 3; The Finnish were even more radical in their approach, by suggesting deletion of all provisions on the conditions for entering alerts. See Council, Document 5709/10/06 (21.09.2006) 4.
\textsuperscript{599} Council, Document 8537/06 (n579).
\textsuperscript{600} Council, Document 5596/06 (27.01.2006).
\textsuperscript{601} SIS II Regulation, art 24(5). This provision was added at the behest of the Commission and the EP. The evaluation report was due to be released in the second quarter of 2016. In correspondence with the Commission (DG Home, Unit B3), I was informed that the report would not be released at least until October 2016.
The relationship between the insertion of an alert into the SIS II and entry ban decisions issued in accordance with the Return Directive merits further attention. The latter is a pan-European legal instrument, the prime objective of which is to establish common standards on the effective removal and repatriation of ‘illegally staying third-country nationals’. The Directive requires Member States to issue return decisions to irregular migrants (Article 6), who are, in principle, granted a period of voluntary departure (Article 7). In cases when no voluntary period has been granted, or if the obligation to return has not been complied with, national authorities may accompany the return decision with an entry ban (Article 11). The modalities of issuing this entry ban, such as the exact conditions of issuance or their length, have been left to the discretionary power of Member States. The ambiguities stemming from the divergent criteria encompassed in the two instruments are acute.

Key in this context is the extent to which the criteria for registering an alert in the SIS II, as analysed above, and the conditions for issuing an entry ban decision may be applied cumulatively, thus offering to Member States unforeseen options, or there must be ‘a mutual limitation of applicability’. A prime example is the lack of explicit reference to proportionality concerns in relation to the issuance of alerts under the Return Directive.

The entry ban criterion has already transformed into a mandatory requirement for EU Member States, in line with the Stockholm Programme. After all, an entry ban will be deprived of its effectiveness if not accompanied by a SIS II alert. Therefore, the Return Handbook of September 2015 recommended the systematic insertion into the system of all entry bans issued under the Return Directive. Along the same lines, the Council invited Member States to take all the necessary measures in order to ensure that entry-ban decisions are always inserted into the system. This development thus constitutes a form of harmonising of the criteria of SIS II alerts as EU Member States cease to lack discretion, at least regarding the requirement to accompany an entry ban with a SIS II alert. Nevertheless, this practice is not aligned – at least formally – to the current wording of the Regulation. Importantly, the mandatory insertion of entry ban decisions seems to suggest a de facto prioritisation of the Return Directive rules over the SIS II Regulation, by circumventing the proportionality clause and the ‘individual assessment’ requirements.

---

603 Meijers Committee, ‘Note on the coordination’ (n597).
604 ibid 4.
605 Return Directive, art 11(2).
607 Commission, ‘Recommendation establishing a common “Return Handbook” to be used by Member States’ competent authorities when carrying out return related tasks’ C2015 6250 final.
Finally, the erosion of the proportionality criterion is well under way; in the aftermath of the Brussels attacks in March 2016, the Commission stated that ‘Member States should enter alerts into the system relating to all measures involving expulsion, refusal of entry or removal of persons from the territory of a Member State’.  

**ii) Beneficiaries of EU law**

Under the pre-existing Schengen acquis, the position of third-country nationals who are beneficiaries of EU law was unregulated, which meant that they were treated no differently to other third-country nationals. Article 25 of the Regulation codifies the case law of the CJEU and stipulates that data on third-country nationals who are entitled to move freely in the EU pursuant to Directive 2004/38/EC can be registered into the system in conformity with the rules adopted in implementation of the Directive. In case of a ‘hit’, the Member State executing the alert must consult immediately the issuing Member State through SIRENE in order to decide, without delay, on the action to be taken. The relevant alert shall be deleted, if the registered person acquires citizenship, as soon as the Member State issuing the alert becomes aware that the person acquired the citizenship.

**iii) The ‘banned’**

Sanctions Committee of the Security Council of the United Nations, against whom different sanctions may be imposed, including a travel ban. Article 26(2) further inserts a derogation to the rule that an alert cannot be entered unless it contains information on the name and sex of the person, a reference to the decision giving rise to the alert and the action to be taken. However, it is unclear how persons listed on terrorist lists could be registered without their names or reference to the action to be taken, unless the intention is that Member States register these persons on the basis of their biometrics. In relation to this category, an individual assessment is not necessary, therefore Member States are obliged to enter the alerts with no discretion. Nevertheless, Article 21, requiring the registration of an alert only when the case is adequate, relevant and important enough, still applies. But, it is hard to imagine a situation when a Member State will exercise such discretion with regard to terrorist lists. As for the Member State responsible for registering, updating and deleting these alerts on behalf of all Member States, Article 26(3) stipulates that it would be designated at the moment of the adoption of the relevant measure. The Parliament had suggested that these should be entered by the Member State holding the Presidency of the mixed committee, which is the current practice.

The interest in alerts on travel bans has recently grown. With a view to reviewing the rules on entering, amending and deleting the travel ban alerts, the Council called for the setting up of a coordination mechanism at EU level for the implementation and follow-up of its decisions on restrictive measures with regards to the alerts. In the aftermath of the Paris attacks of November 2015, Commissioner Avramopoulos stated that a planned review of travel bans is in the pipeline. To the best of my knowledge, this issue has not yet materialised into a concrete proposal.

d) Retention period

According to Article 29 of the Regulation, alerts on third-country nationals shall be stored ‘only for the time required to achieve the purposes for which they were entered’.

614 Brouwer (n17) 97.
615 Peers, EU Justice and Home Affairs Law (n475) 205.
617 Council, Document 11205/12 (15.06.2012) ¶23.
618 Council, Document 17112/13 (29.11.2013). See also Council, Documents 7285/15 (22.04.2015); 10093/15 (23.06.2015).
620 The set-up of a coordination mechanism is discussed in Council, Document 10441/16 (28.06.2016).
As a general rule, the necessity for keeping alerts on individuals registered in SIS II must be reviewed after three years, but Member States may set shorter retention periods where necessary. After that period, alerts must be either deleted or kept if the Member State that issued the alert has notified, based on a comprehensive individual assessment, that the extension of an alert in SIS II is necessary. The proposal envisaged automatic deletion of the alerts after five years, and the Parliament countered with a three-year retention period, which could be prolonged two more years. However, the final text retained the same timeframe as under CISA rules.

e) Access to the data

Article 27 of the Regulation sets out the authorities granted access to the alerts regarding third-country nationals. In a wording that mirrors Article 101 CISA, these authorities are exclusively those responsible for identifying third-country nationals for the purposes of border control and for carrying out police and customs checks within the territory of the Member States, as well as the ‘designated authorities’ coordinating such checks. Furthermore, the provision regarding access by national judicial authorities, as agreed in Regulation 871/2004, has been integrated into the text. Additionally, and by way of derogation, access is granted to national authorities responsible for issuing visas, examining visa applications and issuing residence permits. Access by these authorities to third-country nationals’ data is restricted in that it may take place only for the purpose of refusing entry or stay in a Member State’s territory, and any other use shall be considered as misuse under the national law of each Member State. Pursuant to Articles 27(4) and 31(8) of the Regulation, each Member State is required to send a list of the competent bodies authorised to conduct searches within the system, which are published in the Official Journal of the EU and updated when necessary.
These authorities and their access are, as the EDPS has pointed out, subject to a ‘double test’; access must be granted to authorities that comply with both the overall purpose of the database and the specific purpose of each alert.\textsuperscript{632} As a result, these authorities have a \emph{de facto} use limitation for these data, since they can, in principle, only have access to perform a specific executive action.\textsuperscript{633} Finally, as for the possibility of transferring to third parties, according to Article 39 of the Regulation, these are prohibited.

It must be noted that access to SIS II was originally reserved for the authorities responsible for control of persons at the external borders of the Member States and the authorities responsible for issuing visas and residence permits.\textsuperscript{634} No reference was made to access by national judicial authorities, as that was regulated already. Furthermore, consultation of the alerts was to be allowed to those authorities responsible for identifying a third-country national staying illegally in the Schengen territory pursuant to the Return Directive.\textsuperscript{635} In addition, asylum authorities would access the system in order to determine whether an asylum applicant had stayed illegally in another Member State, or represented a threat to public order or internal security.\textsuperscript{636} The EDPS criticised that suggestion,\textsuperscript{637} and in the end this reference was dropped. Moreover, during the negotiating phase, the Council desired that all the authorities enabled to introduce data should have access to the system and proposed a last-minute change in this respect,\textsuperscript{638} which was, however, rejected by the Parliament.\textsuperscript{639} Despite this turn of events, the possibility of further extending access to the authorities registering alerts has not been excluded. In this respect, it has been noted that:

‘access for authorities which enter data into the SIS II is an important issue related to the safeguarding of the area of freedom, security and justice and that this question will require further examination, including on the possibility to submit new legislative proposals on this subject’.\textsuperscript{640}

\begin{thebibliography}{99}
\bibitem{632} EDPS, ‘Opinion on SIS II proposals’ (n352) 44.
\bibitem{633} ibid.
\bibitem{634} Commission, ‘Proposal for SIS II Regulation’ (n553) art 17.
\bibitem{635} ibid art 18(1).
\bibitem{636} ibid arts 18(2), 18(3). This provision disappeared from the final text perhaps because the negotiated VIS allowed access to asylum authorities. Brouwer (n17) 101.
\bibitem{637} EDPS, ‘Opinion on SIS II proposals’ (n352) 44-5.
\bibitem{638} Council, Document 5709/10/06 REV 10 ADD 1 (29.09.2006).
\bibitem{639} Council, Document 14296/06 (27.10.2006) 3.
\bibitem{640} Council, Document 14490/06 (30.10.2006) 2.
\end{thebibliography}
f) Interlinking of alerts

Another key addition in the SIS II regime is the possibility to interlink different alerts entered into the system.\(^\text{641}\) This essentially means that when an alert is registered in the database, a link to another alert on one or more persons or objects registered in the system may be added,\(^\text{642}\) thus establishing a relationship between the two. National authorities are not required to provide a reason why they created the alert as long as ‘there is a clear operational need’.\(^\text{643}\) Links between two alerts do not influence the rights of access of the relevant authorities, as bodies with no right of access to certain categories of alerts shall not be able to see the substantive content of the linked alert to which they do not have access.\(^\text{644}\) If a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or international obligations, Article 37(6) points out that it may take the necessary measures to ensure that there can be no access to the link from its national authorities.

There have been reported no less than 45 examples of possible combinations of alerts.\(^\text{645}\) In respect of undesirable third-country nationals, alerts may be linked to other entries regulated by the SIS II Decision in the following situations:

a) An EU national wanted for arrest based on an EAW related to a convicted companion who should be refused entry;\(^\text{646}\)

b) Family members in respect of whom SIS II alerts have been registered;\(^\text{647}\)

c) A third-country national’s parent who should be refused entry related to a missing child (third-country national);\(^\text{648}\)

d) A third-country national to be refused entry and the possibility of them being a witness in an illegal immigration case;\(^\text{649}\)

e) A husband of a convicted criminal to be refused entry whose wife is a suspected terrorist;\(^\text{650}\)

f) A third-country national to be refused entry who is also a suspect in an illegal immigration case;\(^\text{651}\)

\(^{641}\) SIS II Regulation, art 37. Compare with recital 19 of the Proposal for the SIS II Regulation where the Commission did not provide details on such interlinking, as these aspects ‘cannot be covered exhaustively by the provisions of this Regulation due to their technical nature, level of detail and need for regular update’.

\(^{642}\) Brouwer (n17) 101.

\(^{643}\) SIS II Regulation, art 37(4).

\(^{644}\) SIS II Regulation, art 37(3).


\(^{646}\) Art 95+art 96 CISA.

\(^{647}\) Art 96+art 96 CISA.

\(^{648}\) Art 96+art 97 CISA.

\(^{649}\) Art 96+art 98 CISA.

\(^{650}\) Art 96+art 99 CISA.
g) A third-country national to be refused entry using his/her own car, boat or aircraft, and

h) A third-country national to be refused entry using stolen identity documents.

**g) Individual rights**

The rights of the individuals in respect of whom alerts are recorded in the system are set out in Articles 41-3 of the Regulation. These include a right of access, correction of inaccurate data and deletion of unlawfully stored data, a right of information and a right to seek compensation for unlawful registration in the SIS II. The right of access is restricted when indispensable for the performance of a lawful task in connection with an alert, or for the protection of the rights and freedoms of third parties. An important improvement in the SIS II involves the right to information as provided in Article 42 of the Regulation. Under the revised regime, third-country nationals who are subject to an alert are to be informed about, amongst other things, the identity of the controller, the recipients of data, the existence of the right of access and rectification, as well as about the purpose of processing. This information must be provided in writing, together with a copy of, or a reference to, the national decision giving rise to the alert. However, this right is subject to numerous exceptions, such as when ‘the provision of information proves impossible or would involve a disproportionate effort’, or where national law allows for the right of information to be restricted, in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

---

651 Art 96+art 99 CISA.
652 Art 96+art 99 CISA.
653 Art 96+art 100 CISA.
655 SIS II Regulation, art 41.
656 ibid art 41(4).
658 SIS II Regulation, art 42(2)(a)(ii).
659 ibid art 42(2)(c).
h) Supervision

The SIS II Regulation stipulates a system of two-layered supervision, whereby the Management Authority (eu-LISA) is checked by the EDPS and national supervisory authorities – essentially national data protection authorities (DPAs) – are responsible for the NSIS II. By reference to Article 28 of the Data Protection Directive, the powers granted to national DPAs are rather extensive, including investigative tasks, intervention, as well as checking the lawfulness and engaging in legal proceedings. A key rule is set out in Article 47, according to which the powers of the EDPS are retained in case the Commission delegates its responsibilities.

4.2 Step four: Additional features in response to the phenomenon of ‘foreign fighters’

The full integration of fingerprints as a form of identification of third-country nationals is not the sole prospective addition to the functionalities of the SIS II. As I have noted elsewhere, the database has been on the front line in the wake of terrorist events, and the current phenomenon of the so-called ‘foreign fighters’ has reinforced calls for further exploitation of the SIS II capabilities. In addition to growing efforts concerning the insertion of alerts on discreet checks, EU nationals will soon be subjected to enhanced checks at the external borders including inter alia systematic consultation of the SIS II. In April 2016, the Commission codified further possible ways of expanding the functionalities of the SIS II. Aspects under scrutiny include: the creation of alerts relating to irregular migrants subject to return decisions; the use of facial images for biometric identification on top of fingerprints; the automatised transmission of information on a hit following a check; the storing of information on discreet and specific check alerts in the system; and the creation of a new alert category on ‘wanted unknown persons’ linked to forensic data existing in national databases,

663 Commission, ‘Stronger and smarter information systems’ (n585) 7-8.
such as latent fingerprints. In addition to these changes, the Council has expressed its desire to grant Europol access to the SIS II in full, including immigration alerts.665

5. Evaluation of the SIS II in light of Article 7 EUCFR

5.1 Application of Article 7 EUCFR

The establishment and operation of the SIS (and SIS II) interacts with the right to private life in a variety of ways. Firstly, as highlighted in Chapter 1, the ECtHR has repeatedly emphasised that the systematic collection and storage of personal data by public authorities falls within the realms of protection under Article 8 ECHR. Subsequent use of the data on the basis of enlarged access amounts to a separate interference with privacy. In the case of the SIS II, national competent authorities must register alerts, comprising of a series of personal data – including biometrics – in order to prevent future access of unwanted third-country nationals to the Schengen territory.

Secondly, under the current regime, the system enables the systematic processing of photographs and fingerprints, which, as noted in the Introduction, can be considered as sensitive data. In S and Marper, the ECtHR took note of the special nature of fingerprints, the retention of which ‘cannot be regarded as neutral and unequivocal’, whereas in Schwarz, the CJEU considered the collection and storage of fingerprints in EU passports as falling within the scope of privacy protection. Thirdly, the registration of an alert entails that the person concerned will, in principle, be precluded from entering the Schengen area. In that sense, it interferes with the right to private life in the form of a person’s freedom of movement. As Brouwer has pointed out, this is especially the case when controls on persons are accompanied by practices embarrassing for travellers, such as taking a person aside, interrogating, collecting biometric data and carrying out body searches.667

It must be further noted that the persons concerned cannot be considered as providing their consent for the registration and processing of their data within the SIS II. Firstly, considering that the right to information can be curtailed on multiple grounds, it is evident that in many cases the person concerned will not even be aware of the

666 S and Marper v UK (n194) ¶84.
667 Brouwer (n17) 174.
existence of an alert in their respect. Furthermore, Article 36 of the SIS II Regulation provides that in cases of misused identity, the person whose identity has been misused may be registered in the system on the basis of their explicit consent. *A contrario*, in all other cases, the persons concerned have not provided their consent.

5.2 Essence of privacy

*Schrems* is the sole case where the CJEU has elaborated on the ‘respect of the essence’ criterion of Article 52(1) EUCFR, and set the bar high by opining that generalised access to the content of electronic communications goes to the core of privacy. Due to the sensitive nature of biometric data, and the stigmatising effect of treating information on non-criminals in the same way as that of criminals, as highlighted in *S and Marper*, it is arguable that generalised and indiscriminate collection and further processing of biometric data in massive databases compromises the essence of privacy when this information is used in a multiplicity of contexts and involves unsuspected individuals.\(^{668}\) In this regard, Ojasen has rightly pointed out that the more systematic and wide the processing, the closer it can be seen as getting to the nucleus of privacy.\(^{669}\) In the present case, the registration of biometric data involves third-country nationals whose personal conduct has been found as violating national laws – criminal or administrative in nature. Consequently, the essence of privacy seems to be respected, even though the registration relates to a very large number of persons.

5.3 Objective of general interest

Both European Courts have rarely disputed the legitimacy of the aims pursued by enacted legislation, either at the national or at EU level. According to Article 1(2) of the SIS II Regulation, the, admittedly very broad, purpose of SIS II is twofold: first, to ‘ensure a high level of security’ within the EU AFSJ, and second, to ‘facilitate the movement of persons using information communicated via this system’,\(^{670}\) both of which are long-established aims of the EU. Besides, the first objective is also directly associated with the purposes of ensuring ‘national security’ or the ‘prevention of

---

668 This view is shared by Ojasen, who however, does not reflect further on this issue. Ojasen, ‘Making the Essence’ (n445) 326.

669 ibid 328.

670 Commission, ‘Overview of information management’ (n27) 22.
disorder or crime’ encompassed under Article 8(2) ECHR. Furthermore, Article 6 EUCFR mandates that ‘[e]veryone has the right to liberty and security of person’.

5.4 Is the limitation ‘provided for by law’?

This criterion requires that there is some form of legislation on which the limitation is grounded, and that the legislation bears the qualities of accessibility and foreseeability. The requirement of accessibility is satisfied by the publication of the SIS II Regulation in the Official Journal of the EU. This includes the obligation imposed on Member States to notify the Commission on the list of competent authorities that are granted access to the database, the subsequent publication of the respective lists and the periodic review of these lists is central. However, the lack of obligation for publication of the national criteria at EU level raises concerns, since without that information it is difficult for the individual to foresee under what circumstances their personal data shall be collected, stored and further processed.671 The problem becomes even more acute as in certain Member States, such as Finland, the national criteria are unpublished even under national law.672

The vague wording of the purpose of the database also poses significant legality concerns regarding the gradual transformation of the system from a reporting system into a powerful investigative tool, the full potential of which has yet to be reached. The intertwining of immigration control with security disregards the specificity of the immigration branch of the database as a tool solely for the refusal of entry to, and stay in, the territory of the Member States. In view of the growing convergence of alerts inserted, particularly through interlinking and inclusion of biometrics, which allow for multiple uses, the broad terms in which the purpose of the database is worded is problematic, as it leaves huge leeway for introducing further new functionalities which are unforeseeable to the individuals concerned. The future access to SIS II data by Europol is another indication of the intelligence-gathering direction of the system.

Moreover, the interlinking as such does not allow the individual concerned to foresee how their information shall be further used. Finally, as regards to the inclusion of biometric identifiers into the system, it is true that the Regulation does not include

671 Peers, EU Justice and Home Affairs Law (n475) 209.
detailed rules on the collection and storage of such data, but the SIRENE Manual contains a series of provisions regulating different instances of biometric data processing. In line with the relevant European Courts case law, I consider that both the insertion of biometrics and the interlinking of alerts are more closely related to the proportionality test, analysed below.

5.5 Proportionality test

The inherent flexibility of the SIS II in its design renders the assessment of the proportionality of SIS II immigration provisions challenging. As the SIS Joint Supervisory Authority noted already in 2004:

'It is difficult to see how there can be a proper assessment of the potential implications of the SIS II when its development is to be so flexible that it is unclear what form the system will ultimately take … [and] must also make it more difficult for those developing the system to take account of the principle of proportionality.'

Be it as it may, the appropriateness of registering alerts in general as a means of preventing and refusing the entry or stay of undesirable third-country nationals cannot be contested as long as both the modalities of storage and each specific registration are proportionate to the aim pursued. However, it is noteworthy that despite the overzealous registration of alerts on third-country nationals over the years, the number of ‘hits’ remains relatively low. Furthermore, proportionality concerns are raised in relation to numerous aspects of the database, namely its personal scope, the processing of biometrics, the retention period, the authorities granted access to the alerts and the interlinking between alerts registered under different legal bases, which are examined in turn below.

5.5.1 Personal scope

In relation to the personal scope of the database, the SIS II stores alerts on third-country nationals who must be banned from entering the Schengen territory on the basis of their personal conduct. Article 24 of the Regulation leaves wide discretion to national

---

674 See n565.
675 Schengen JSA, ‘Opinion on the development of the SIS II’ (19.05.2004) 3.
676 See above, Section 4.1.1.
authorities, by listing three categories of persons who may be entered into the system, however, the list is by no means exhaustive. In *Digital Rights Ireland*, the *en masse* and indiscriminate collection and storage of personal information were influential in making the Data Retention Directive invalid. In principle, the registration of alerts on undesirable third-country nationals in bulk seems to be prevented by the existence of the general proportionality clause set out in Article 21 of the Regulation, and the obligation to conduct an individual assessment before the insertion of an alert.

These safeguards, however, are insufficient in multiple respects. As it has already been pointed out, the lack of harmonised criteria across Member States signifies that national authorities may have very divergent understandings of the circumstances triggering a SIS II alert. This key problem of the database reflects not only on the significant issue of the person being barred from the Schengen territory, thus restricting their free movement and, perhaps, obstructing in maintaining personal relationships developed there, but also to the mere storage and use of their data within a centralised database. In other words, privacy concerns start from the initial national decision to register an alert in the system on the basis of national criteria. It has already been noted that in the first years of the SIS operation, wide discrepancies were evident as regards to the recording of alerts triggered by breaches of national immigration laws or merely by failed asylum applications. It has been reported that a significant percentage of alerts were unlawful; for instance, in France 40% of cases checked by the French DPA and between 10-50% in Germany. Kabera Karanja goes as far as to note that the rate of alerts registered for unlawful reasons has been as high as 77%. Over the course of time, certain issues seem to have been resolved. However, a query regarding the grounds for registering alerts confirms that wide divergences persist; in certain Member States the threshold for entering alerts is significantly higher than in others, for instance in Lithuania, where the refusal or annulment of a visa and the refusal or withdrawal of a residence permit triggers a SIS II alert, whereas other Member States follow the categories set out in the Regulation. In numerous States an expulsion decision (return) is automatically accompanied by an alert. These divergent standards signify that individual cases are treated differently depending on the national implementation, in other words, depending on where the person concerned is situated the extent to which their privacy rights may be violated due to a disproportionate decision regarding the registration of a SIS II alert significantly varies.

---

677 Brouwer (n17) 379, 427-8.
678 Kabera Karanja (n29) 216.
680 EMN, ‘Ad Hoc Query on procedures’ (n672).
681 ibid.
The mandatory registration of entry bans into the SIS II is a significant step towards the harmonisation of national criteria. However, it is not without problems. Apart from the fact that, at present, this development is currently not supported by the wording of the text, as it has been already pointed out, the relation between the Return Directive and the insertion of an alert is obscure and leads to a significant watering down of the protection afforded by the SIS II Regulation. The obligation of national authorities to accompany entry bans with a SIS II alert inevitably raises the question of what are the conditions for issuing entry ban decisions against irregular migrants and how these have been transposed at the national level. According to Article 11(1) of the Return Directive, an entry ban must be issued where a return decision was ordered without a period for voluntary departure being granted, or where the obligation to return has not been complied with. In other cases, an entry ban may be issued. Therefore, entry bans may be implicitly issued even if a period for voluntary departure has been granted and even if the return decision has been complied with.\textsuperscript{682} Hence, there is no objective and standardised mechanism, as Member States have been granted wide discretion on this issue. This discretion is reflected in the more recent evaluation of the Return Directive, whereby in no less than 11 Schengen States an entry ban is automatically issued alongside a return decision, whereas in 14 countries irregular migrants are issued with an entry ban on the basis of the criteria set out in Article 11(1).\textsuperscript{683} In three states only the entry ban decision is taken on a case-by-case basis.\textsuperscript{684} This means that in a significant number of Member States, SIS II alerts are registered in bulk and on the basis of automaticity solely because third-country nationals have been issued return decisions, and with minimum guarantees that the seriousness of each case has been individually evaluated.\textsuperscript{685} Whilst this does not pose any concerns as regards to compliance with the Return Directive, it results in circumventing the procedural safeguards prescribed in the SIS II Regulation. Importantly, this implies that, at least in certain Member States, the entry of SIS II alerts involving irregular migrants carries the characteristics of massive registration without any limitations, exceptions or distinctions, thus raising serious proportionality concerns. The possibility in the future to enrol all return decisions in the system, as is currently being advanced, enhances the risk of further watering down of the SIS II standards, and leads to automatic storage of

\textsuperscript{682} Peers, EU Justice and Home Affairs Law (n475) 570.
\textsuperscript{684} ibid.
personal data of basically all irregular migrants irrespective how serious the violation of immigration law has been. It may even apply in cases where the irregular migrant has left a national territory voluntarily, which is disproportionate in view of the personal conduct of the person concerned.

Therefore, the harmonisation of criteria for entering alerts may progressively result in generalised and indiscriminate storage of personal data of all irregular migrants, thus invalidating the guarantees envisaged in the SIS II Regulation. *Ex post* rectification of the conditions for issuing entry ban decisions is not sufficient, since in the meantime, in a number of cases personal data will be stored in the system even though their registration may have been disproportionate. The harmonisation of criteria for entering alerts concerning irregular migrants is imperative as long as it is accompanied by clear rules of the measures to which the SIS II is linked, such as the Return Directive, including provisions on the relationship between the two provisions. Otherwise, it is not guaranteed that alerts are issued solely when they are objectively justified in light of the degree of criminality or seriousness of the breach of national immigration laws.

Furthermore, a third-country national who has committed an offence carrying the penalty of imprisonment of more than a year may be registered in the system, however the lack of specific categories of offences justifying an alert means that third-country nationals may be registered even for minor offences as long as the threshold of one year imprisonment is met.\(^686\) Moreover, it is recalled that an alert regarding a person who is suspected for committing an offence carrying such a penalty is entered on the basis of clear indication, as opposed to the higher threshold of clear evidence, allowing wider discretion to Member States.

Finally, the proportionality of registering alerts on UN and EU travel bans into the system is inextricably linked to the legality of the procedure leading to the imposition of the terrorist sanction. A rich body of academic literature has dealt with these issues, particularly the compliance with due process rights, with commentators criticising the secrecy of the procedures both at UN level and at EU level, and the lack of clarity on the criteria on the basis of which third-country nationals are listed as terrorists.\(^687\) The CJEU *Kadi* judgments are landmark in this respect for highlighting the need for

---

686 Brouwer (n17) 440.
rigorous judicial review in light of the significant impact of such sanctions. Furthermore, in *Nada v Switzerland*, the ECtHR engaged *inter alia* with the question whether the imposition of a travel ban violates with the right to private life. The Court opined that the restrictions imposed on the applicant’s freedom of movement for a considerable period of time did not strike a fair balance between his right to privacy on the one hand, and the legitimate aims of the prevention of crime and the protection of Switzerland’s national security. In reaching this conclusion, the Court took note of the fact that allegations against Mr Nada were clearly unfounded, but that information was not communicated until years later. In the case of the SIS II, the lack of specific guarantees and the automaticity of registration raise concerns, which are enhanced by the possibility of entering incomplete alerts.

### 5.5.2 Inclusion of biometrics

A second issue raising proportionality concerns is the inclusion of biometrics. Admittedly, their deployment will enable individuals in respect of whom there is apparently an alert to ‘clear their names out’ in so-called ‘John Smith’ cases and may also allow the interception of persons who use fraudulent documents to circumvent the SIS II procedure. Strikingly there is no further elaboration on the benefits and risks of this function, as no impact assessment was conducted and neither was an explanatory memorandum attached to the proposal. What appears to have been the driving force is the fact that the Eurodac was already processing fingerprint data on a large-scale for the identification of asylum seekers and irregular migrants, and that agreement had already been reached regarding the collection and storage of biometrics within the VIS. This argumentation *a minori ad majus*, according to which biometrics should be added to the SIS II, which is security-oriented, because other databases which were not conceived as

---


690 Ibid ¶199.

691 Ibid ¶188.

692 House of Lords, ‘SIS II: Evidence’ (n613) 14.


694 EDPS, Opinion on SIS II proposals’ (n352) 42.

695 This was criticised by the EDPS and the Article 29 DPWP, ‘Opinion 6/2005’ (n585) 7.
primary law enforcement tools process, is neither sufficient nor relevant for adding such important functions. Neither is the fact that the addition of biometrics would facilitate future interoperability between these systems.

The lawfulness of the addition of photographs and fingerprints in the SIS II is highly doubtful. This is because Article 40 of the SIS II Regulation proscribes the processing of sensitive data within the SIS II. A combined reading of this proviso with the rules on the inclusion of biometrics suggests that the EU legislator does not consider these forms of biometric identifiers as constituting sensitive data. Until recently this issue was not a setting stone, although several sources have observed that both photographs and fingerprints may reveal ethnic and racial origin and, particularly in relation the SIS, the EDPS has highlighted the ‘inherently sensitive nature of biometric data’. With the adoption of the General Data Protection Regulation, this issue is clarified in that biometric data have been added to the list of special categories of personal data, alongside data revealing racial and ethnic origin and genetic data, the processing of which is prohibited where processed to ‘uniquely identify a person’.

The growing use of biometrics in large-scale systems seems to be based on an over-estimated role of biometric identifiers. However, depending on the different functions for which they are deployed, and the modalities of their storage, their reliability differs significantly. As Kindt has eloquently observed, when biometrics are centrally stored, the error rates are impacted by the number of persons subjected to the system. Therefore, the larger the system, the more possible a ‘hit’ is based on an error. The consultation of a system on the basis of latent fingerprints – that is incomplete fingerprints found in a crime scene – is also a factor influencing the reliability of the system.

Furthermore, the centralised storage of biometrics as such may grow the appetite for their use for other purposes than the ones for which they were originally collected and stored, and is prone to attacks. As it was highlighted in Schwarz, the storage of two fingerprints in the medium of an EU passport was found proportionate, because

---

696 Article 29 DPWP, ‘Working Document on biometrics’ (n21) 10; Kindt lists a series of studies conducted according to which fingerprints may reveal racial or ethnic origin as well as health problems. Kindt (n13) 140-1.
697 EDPS, ‘Opinion on the SIS II proposals’ (n352) 44.
698 General Data Protection Regulation, art 9(1). According to art 9(2), processing is allowed when inter alia ‘necessary for reasons of substantial public interest’. The SIS II rules though must prevail as lex specialis.
699 EDPS, ‘Opinion on SIS II proposals’ (n352) 44.
700 Kindt (n13) 59.
702 Kindt (n13) 651.
these fingerprints were used solely to verify the identity of the passport owner – therefore as an additional authentication factor – and because these were not stored centrally in a large-scale database. In the case of the SIS II, these characteristics are missing. On the contrary, the centralised storage of biometrics signifies that the individual concerned loses control over the storage and possible re-uses of their sensitive personal data. As the database is subject to consecutive reconfigurations under the ‘umbrella’ purpose of maintaining security, the danger of biometrics being used for purposes other than the ones for which they were originally collected and stored is heightened. As two authors have noted, biometrics could be used in the course of investigations and enable speculative searches (the so-called ‘fishing’ expeditions) whereby the persons stored in the system constitute a suspected population. Central in this respect is the already existing possibility to use biometrics as a search key in order to reveal links to other alerts. The recent Commission report on the readiness and availability of fingerprints for identification purposes confirms these fears, as it is stated that a comparison of fingerprints to those already stored ‘might identify links with other alerts.’ Therefore, biometrics are not merely collected and stored to ‘sort out’ the ‘welcomed’ from the ‘unwanted’, but also to enhance the investigative powers of national law enforcement authorities. In light of these considerations, the consequences for third-country nationals may be significant. By contrast to Schwarz, where the CJEU observed that a mismatch in respect of an EU citizen would merely draw the attention of national authorities to the case, leading to a second round of checks, a possible error in SIS II would entail, in principle, refusal of entry into the Schengen territory, or refusal of granting a visa or a residence permit. Furthermore, it could trigger administrative procedures related to expulsion, or in relation to violations of national immigration rules, or even initiation of prosecution, particularly if the fingerprints are wrongfully linked to other alerts. The third-country national in question could be detained in the meantime.

Even if it were to be accepted that the processing of biometric identifiers in a large-scale database is necessary and appropriate, by mandating the collection and storage of both a full set of fingerprints and a digital photograph, the Regulation has exceeded its limits of discretion in relation to the aims pursued, deepening the surveillance of movement imposed on individuals concerned. For instance, in a study for the EES, it has been observed that two or four fingerprints are sufficient for reliable

703 Schengen JSA, ‘Opinion on the proposed legal basis’ (n570) 9.
704 Hayes (n521) 4; Baldaccini (n23) 38.
705 Commission, The availability and readiness of technology’ (n587) 7.
Finally, the lack of rules within the Regulation regarding the procedure of collection and storage of data, the need to take into consideration the age of the individual as well as the different nature of categories of persons against whom alerts are inserted (criminals, suspects, irregular migrants), as mandated in *S and Marper*, also raise proportionality concerns. Treatment of irregular migrants who are merely subjected to a return decision should not receive the same treatment as third-country nationals who have been convicted of a criminal offence.

### 5.5.3 Retention period

Another central aspect is the retention period of alerts. In *S and Marper*, the ECtHR condemned the indefinite storage of biometrics of persons who were not convicted of any criminal offence. Furthermore, the Court demanded a differentiated treatment depending on the age of a person concerned or whether they had been convicted of an offence or not. Moreover, in *Digital Rights Ireland*, the Grand Chamber called for keeping the retention period as short as possible, based on the purpose of the data. As regards the SIS II, the EU legislator has opted for granting broad leeway to Member States by requiring, in principle, deletion of the data after three years subject to review, but without prescribing a specific retention period. The present case differs from these judgments in that the storage – at least partly – involves persons with criminal convictions as well as persons whose conduct – irregular entry or stay – may constitute a criminal offence in many Member States. However, it also involves individuals who are merely suspected of being about to commit, or having committed, an offence. Furthermore, it is arguable that the violation of immigration law is qualitatively different from other criminal offences. In this context, a maximum duration for retaining the data is necessary in order to avoid wide discrepancies at the national level, which, in fact, are profound. For instance, in several Member States, the maximum retention period is five years, whereas in others it is 10 years, or even up to 20. The minimum term equally ranges from one month to five years. In three Member States,

---

708 The fact that immigration offences constitute criminal offences was pointed out to me in an informal discussion with a Commission official (Brussels, November 2014). On the need to revise policies attaching to immigration breaches criminal penalties see Thomas Hammanberg, ‘It Is Wrong to Criminalise Migration’ (2009) 11(4) *European Journal of Migration and Law* 383.
709 EMN, ‘Ad Hoc Query on procedures’ (n672).
there is no maximum retention period indicated in law. The issue becomes more complicated following the mandatory registration of entry bans into the system, as the maximum length of entry bans is left open in the Return Directive,\(^{710}\) and in certain countries the duration of an entry ban is indefinite or not specified in law.\(^{711}\) Therefore, in view of the link established between an entry ban and a SIS II alert, it is only logical that the relevant alert cannot but be renewed pending the ban, thus leading to particularly extensive and disproportionate storage of data. In this context, clear time limits are needed, which should further differ depending on whether the alert is registered on public policy, public security or national security grounds, or due to breaches of national immigration provisions. Further guidelines for national authorities would also be beneficial.

### 5.5.4 Accessing authorities

Article 27(1)(b) of the SIS II Regulation allowing access to authorities responsible for police and customs checks, and for the coordination of their tasks by designated authorities, seems rather vague and allows for disproportionately widening the pool of authorities to agencies entrusted with tasks that are not directly related to the specific aim of refusing entry or stay of third-country nationals, but are more intelligence and investigation-oriented. The case of internal security and intelligence services is key in this respect. During the negotiating phase, the German government proposed amending Article 37 of the SIS II Decision in order to grant national intelligence services access to alerts held in the system, including data on third-country nationals.\(^{712}\) This proposal was rejected by the Parliament.\(^{713}\) However, Article 27(1)(b) implies that access to designated authorities for the purpose of coordinating police and customs checks is allowed. The term ‘designated authorities’ is recurring in the terminology of EU immigration databases and, in principle does not exclude internal security agencies.\(^{714}\) Therefore, it is not improbable that at the national level, Member States include among the agencies having access to the data authorities that were otherwise excluded. This has indeed happened in practice, as the latest list of competent authorities includes bodies

---

710 Note that the Article 11(2) of the Return Directive stipulates that in principle the duration of an entry ban is five years.


712 Council, Document 12160/06 (21.08.2006).

713 Council, Document 14296/06 (n639) 3.

714 See Chapter 3, Section 3.3.1.
entrusted with internal security. Another vague provision is Article 27(2) of the SIS II Regulation allowing access to national judicial authorities ‘and by their coordinating authorities’, because it leaves unclear which authorities fall exactly under this description. The publication of a list of competent authorities does not seem to help much. As Geyer has correctly pointed out, the blurring of boundaries regarding the competent authorities is inherent to the system, since it contains both law and border control and immigration law information. It is the need for notification of authorities to the Commission that safeguards the boundaries. Yet, these attempts seem fruitless as Member States are essentially free to designate their competent authorities, and it appears that no EU institution has the power to reject or review the designation communicated by a Member State. This is true; the inclusion of internal security agencies is not the sole example of competent authorities enlisted that seem to fall outside of the scope of Article 27. In the same list, there appear national asylum authorities, which, as mentioned above, were also excluded in the final text.

5.5.5 Interlinking of alerts

Finally, proportionality concerns are raised by the interlinking alerts. This new feature entails the progressive merging of purposes, whereby data recorded in relation to one alert are used for the purposes of other alerts too. As ‘a very typical feature of a police investigative tool’, interlinking is not merely a technological upgrade in the database, but yet another indication of the transformation of the function of the database with significant consequences for the individuals concerned. Supposition and ‘intelligence’ find their way into the database, and ‘criminal gangs’, ‘crime families’, ‘illegal immigration networks’ and, presumably, suspected ‘terrorist networks’ may even be registered en masse. As the EDPS has eloquently observed:

‘[T]he person is no longer “assessed” on the basis of data relating only to him/her, but on the basis of his/her possible association with other persons.

---

715 Notices of Member States (n631); These are: Latvia, Estonia and Poland.
716 Brouwer (n17) 100.
718 Ibid.
719 These are Bulgaria, Greece and Austria.
720 EDPS, ‘Opinion on SIS II proposals’ (n352) 46.
721 Hayes (n521) 5.
Individuals whose data are linked to those of criminals or wanted persons are likely to be treated with more suspicion than others.\footnote{722} Creating links between alerts may lead to situations where persons who were previously innocent become connected with criminals or criminal networks with adverse affects on their status.\footnote{723} A prime example in this respect would involve alerts on irregular migrants linked to those on traffickers or smugglers, possibly leading to further stigmatisation.\footnote{724} The proportionality concerns become more acute when considering the amount of unlawfully registered alerts in view of the lack of harmonised criteria.

Furthermore, even though according to Article 37(3) of the Regulation, national authorities that would normally not have access to the system will not be able to see the link, as Mitsilegas has noted, this does not mean that they do not see the existence of a link.\footnote{725} Furthermore, given that in numerous Member States competent authorities are defined in rather broad terms, and many authorities have access to more than one category of data (e.g., national police), this safeguard may prove less useful than originally intended.

\section*{6. Conclusion}

This Chapter sought to analyse the privacy challenges posed by establishment, operation and possible reconfiguration of the SIS II. It has been observed that the system engages with the right to private life in multiple ways, not least because it involves the systematic collection and storage of a series of personal data, including biometrics. The recording of an alert as such signifies that the person concerned is, in principle, obstructed from free movement, and may be further restricted in maintaining personal relationships and ties with persons located in the EU. By mapping the historical and legislative framework from its initial conceptualisation through to the latest proposals, it became evident that the SIS II has been progressively morphed from a reporting system into a powerful intelligence database. The chronicle of a transformation foretold has been based on four key changes in the operation of the system, all of which raise serious proportionality concerns.

\footnote{722} ibid.  
\footnote{723} Boehm (n32) 266.  
\footnote{724} EDPS, ‘Opinion on SIS II proposals’ (n352) 46.  
\footnote{725} Mitsilegas, EU Criminal Law (n458) 241.
The first change has been the gradual expansion of the scope *ratione personae* via both the introduction of harmonised criteria through the back door at the lowest common denominator, and lowering the threshold for registering alerts. Automaticity that was prevented through the insertion of a proportionality clause has been deployed at the national level, and progressively endorsed at EU level in a bottom-up process with minimum transparency and scrutiny. The lack of clear rules as regards to the relationship with the Return Directive and the discretion allowed to national competent authorities entails the risk of registrations of irregular migrants in bulk without due consideration of their personal circumstances. The second change has been ‘methodological’. Caught in between a dual structure and the need to ensure a high level of security, the SIS II has been inevitably influenced by the growing trend of processing biometric data, which is primarily a security and crime governance method. This change in surveying the risk of irregular migration is not unproblematic. Not only are biometric identifiers sensitive data, the processing of which is explicitly forbidden by the SIS II Regulation, but also their use for identification purposes is far less reliable, and may have significant repercussions for individuals who are wrongly identified. In addition, their recording enables processing for purposes other than those for which they were initially collected, such as ‘fishing’ expeditions, particularly since they will be used as a search key to uncover links to other alerts. The interlinking of alerts is the third change, and is indicatory of merging of purposes, whereby a person’s data becomes relevant in multiple contexts. Finally, the authorities granted access to the system are directly linked to the introduction of collecting biometric data. Over the years, the SIS II has opened up to national judicial authorities and internal security agencies, whereas in the future Europol may also gain access and get their hand in the irregular migrants’ jar. Coupled with the lack of centralised control on the authorities designated at the national level, the mixed nature of the system seems to be gradually abolished, and the specific purposes for which alerts are issued are further eroded.

Overall, the ‘success’ of the SIS II lies in its flexibility, vague wording and wide discretion to define the outer limits of who constitutes part of the risk population, and be subject to surveillance of their movement. The evaluation of the effectiveness of this expansive preemptive model of immigration control will be published by the Commission in autumn 2016, possibly accompanied by new proposals to materialise the vision of an instrument of maximum potential.\(^\text{726}\) Despite the aforementioned privacy concerns, the SIS II will undoubtedly continue to be considered as the ‘panacea’ for addressing security concerns ranging from counter-terrorism to immigration problems.

\(^{726}\) Council, Document 5968/02 (n551).

At the very least, it targets third-country nationals who have in some way attracted the attention of national administrative or law enforcement authorities due to their misconduct. The VIS, that is examined next, differs in that it stores information on all short-stay visa applicants who are, in principle, unsuspected of any misbehaviour. In effect, the privacy concerns differ as well.
CHAPTER 3. The Establishment of the Visa Information System (VIS): A Decisive Step towards Surveillance of Movement

‘At the time of warnings about the frightening spread of the Mafia as well as terrorist conspiracies, why is the EU going down this blind alley of mass surveillance of the 99.9% of the public which is innocent, when the real need is to target the 0.1% of travellers who might be dangerous or criminal through intelligence-led policing and effective cross-border cooperation between law enforcement agencies?’\(^\text{727}\)

1. Introduction

The VIS is a management tool of the EU instrument of extraterritorial immigration control \textit{par excellence}, the visa.\(^\text{728}\) The system was conceived in the aftermath of 9/11 and was officially set up by Decision 2004/512/EC,\(^\text{729}\) supplemented by Regulation 767/2008.\(^\text{730}\) The underlying logic of the VIS is the mandatory collection, storage and further processing of personal data of all third-country nationals who apply for a short-stay visa. Under the ‘umbrella’ purpose of improving the implementation of the common visa policy, the information recorded is used for a multiplicity of divergent aims such the fight against identity fraud and the enhancement of the EU internal security. The latter functionality is regulated by Council Decision 2008/633/JHA,\(^\text{731}\) which allows under specific conditions, and on an ancillary basis, consultation of visa

\(^{728}\) Elspeth Guild, ‘The Border Abroad – Visas and Border Controls’ in Kees Groenedijk, Elspeth Guild and Paul Milderhoud (eds), \textit{In Search of Europe’s Borders} (Kluwer 2002) 94.
data by law enforcement authorities and Europol in order to prevent, detect and investigate terrorist acts and other serious criminal offences.

This Chapter focuses on the privacy concerns raised by the setting up and operation of the VIS. Firstly, I briefly outline the development of the EU common visa policy within the auspices of which the VIS is placed and discuss the role of visas that the VIS supports. Then, I provide an overview of the history behind the adoption of the legislative framework, which is then analysed and assessed in light of privacy.

2. An outline of the EU common policy on short-term visas

Visa is the legal title provided by a State to a foreigner, permitting entry, stay, or transit through that State and a key instrument to control and confine mobility concerning the majority of cross-border movements. It is a clear example of what has been termed ‘remote control’, policiing at a distance’, or ‘pre-emptive mobility governance’, whereby States seek to prevent people from reaching their territory without prior permission. Requiring a visa enables States to exercise extraterritorial immigration control in the sense that the encounter between the State authority, or its delegates, and potential border-crossers already takes place at the point of departure of the people on the move. A number of other parameters are intertwined with the imposition of a visa requirement to the nationals of a specific State, with concerns related to irregular migration featuring prominently, since short-term mobility is deemed a primary source of irregular migrants, mainly through overstaying visas. Criminality is also part of the equation. In this context, a visa indicates a speculation encompassing the entire population of a specific country that, since someone originates from there, a certain type of a behaviour, which is frowned upon, is expected. Guild observes that ‘the profile is not based on the individual as such but on a predetermined stereotype of who is a risk’.

733 Didier Bigo and Elspeth Guild, ‘Policing at a Distance: Schengen Visa Policies’ in Didier Bigo and Elspeth Guild (eds), Controlling Frontiers. Free Movement into and within Europe (Ashgate 2005).
735 For an overview see Ryan and Mitsilegas (n2).
737 Guild, ‘The Border Abroad’ (n728) 94.
least partially, removed when the visa is issued, which can be understood as national authorities having been convinced that the person in question is an exception to the rule and is not a risky. 738 A profile of countries is thus constructed accompanied by distrust, fear and suspicion, which, however, may be rebuttable. A central consideration in this respect is the globalisation process, characterised by increased mobility activities, greater connectivity across borders and processes of re-bordering, 739 leading visas to acquire a multi-faceted role.

Visas first became a matter of collective interest among EU Member States within the Schengen cooperation framework. The process of eliminating border controls, as outlined in Chapter 2, entailed that any person who had been admitted for a short-stay or longer-term residence in one Member State would be entitled to freedom of travel once the prospect of internal border checks was removed. 740 Consequently, a common policy on short-term visas had to be established, since a visa issued by one Member State would effectively permit travel to the others as well. 741 CISA contained extensive rules on short-term visas, defined as 90 days per period of 180 days, 742 supplemented by provisions on freedom to travel. 743 At EU level, the Maastricht Treaty inserted Article 100c, empowering the Community to draw up ‘a list of third countries whose nationals must be in possession of a visa when crossing the external borders of the Member States’ (the ‘black list’), and to adopt ‘measures relating to a uniform format for visas’ that would be valid for all Member States. Furthermore, Article K.1 TEU of the then third pillar provided for the adoption of rules on the conditions of entry and movement of third-country nationals, subject to unanimous voting in the Council. 744 With the entry into force of the Amsterdam Treaty, the Schengen acquis was activated in the control of the borders of the EC, which further acquired competence in adopting rules on visas. 745 The incorporation of the Schengen acquis delimited the interest for further developing visa rules, but the 9/11 events gave a fresh impetus to step up cooperation. The versatility of visas is evident in the determination of the criteria for ‘black-listing’ as well as the formation of various strands of EU action in this field. Illegal migration, criminality and international relations feature as the three criteria for creating a risk

738 ibid.
740 Elspeth Guild and Jan Niessen, Immigration and Asylum Law in Europe vol 2 (Kluwer 2001) 17.
742 CISA, arts 9-17.
744 The adoption of ‘black list’ was until 1 January 1996 also subject to unanimous voting and consultation by the Parliament.
profile of countries, which have, however, attracted criticism for their imprecision and discriminatory character. Another key aspect in this regard is the gradual enlargement of the EU, which has led to a growing entanglement of visa policies with the development of neighbouring and, more generally, external policy and accession processes. Furthermore, calls for visa waivers and visa facilitations agreements, coupled with re-admission agreements, have been multiplied in light of the financial benefits of travellers to EU tourism, under the logic that visa restrictions may substantially hinder Member States in reaping the benefits of economic globalisation.

The current EU legal framework on Schengen visas in effect leaves little leeway to Member States to deviate from the prescribed policies, but long-term visas remain regulated at the national level only. Its territorial scope is subject to the following arrangements: the UK and Ireland have almost never opted in to any measure related to visas; Denmark is bound as a matter of EU law by all measures concerning visa lists and a common visa format, and as for the measures building on the Schengen acquis, it can decide whether to opt in, in which case the rules apply as a matter of international law; and Cyprus, Romania and Bulgaria are bound by a limited set of visa rules, since the acquis has not been fully extended to them. For the remaining Schengen Member States, visa rules are fully applicable. Overall, the EU common visa policy comprises ‘black’ and ‘white’ lists of countries, which are periodically revised in view of the, not uncommon, visa waivers; the Visa Code, currently subject to amendment; rules on the visa format; and a huge Schengen-wide database, the VIS.

---

746 Commission, ‘Proposal for a Council Regulation listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement’ COM (2000) 027 final.
750 Steve Peers and others, EU Immigration and Asylum Law vol 3 (Martinus Nijhoff 2012) 1. Post-Lisbon, decision-making rules have been normalised (art 77 TFEU).
751 See n720.
752 Council Regulation (EC) 574/1999 of 12 March 1999 determining the non-EU Member countries whose nationals must be in possession of visas when crossing the external borders of the Member States [1999] OJ L72/2 as amended therein. As of July 2016, 109 countries are included in the ‘black-list’.
754 For the legal framework see Peers, EU Justice and Home Affairs Law (n475) 256-7.
3. The Visa Information System (VIS): A multifunctional tool

3.1 A long history in short

The establishment of the VIS should be viewed in the broader context of the post-9/11 immigration control and counter-terrorism initiatives on the other side of the Atlantic.\(^{756}\) Influenced by the manner in which the attacks took place, the US Government placed an emphasis on ‘border security’\(^{757}\) and on stepping up control on the entry to the US of those who could execute terrorist attacks. An important strand of action involved the widening, and deepening, of information collection and sharing, including the broad application of biometrics,\(^{758}\) as exemplified in the 2002 National Strategy for Homeland Security.\(^{759}\) Terrorist travel was a strong point of emphasis in this respect. Among the series of executive and legislative measures adopted, a National Security Entry-Exit Registration Programme (NSEER) was set up, which combined a new, biometrics-based registration process for travellers to the US who were broadly regarded as potentially risky, with pre-existing databases.\(^{760}\) The NSEER was soon replaced by the US-VISIT Program, which considerably expanded the personal scope of data collection by requiring almost every traveller to be fingerprinted and photographed on an indiscriminate basis under the logic of ‘enrolment’. Although the US-VISIT is further analysed in Chapter 5, it suffices here to mention that it was designed to survey the pre-entry, entry, stay and exit of foreign visitors forming ‘part of a continuum of security measures that begins overseas, when a person applies for a visa to travel to the United States, and continues through entry and exit at US air and seaports and, eventually, at land border crossings’.\(^{761}\)

The convergence between terrorism, security and immigration policies and the emphasis on collection of personal data, particularly from third-country nationals, has been apparent also at EU level. The introduction of the VIS, as Baldaccini has rightly

\(^{756}\) See also Chapter 5, Section 2.


\(^{758}\) As Epstein observes, ‘[b]iometric borders’ were Congress dream of a perfect shield for the homeland’. Charlotte Epstein, ‘Embodying Risk: Using Biometrics to Protect the Borders’ in Louise Amoore and Marieke de Goede (eds), *Risk and the War on Terror* (Routledge 2008) 180.


\(^{760}\) Epstein (n758) 181-2.

observed, was ‘a direct consequence of the terrorist attacks’ of 9/11. Already since the extraordinary JHA Council meeting of 20 September 2001, Member States requested ‘rigorous procedures in issuing visas’ and called upon the Commission to submit proposals for the establishment of a network for information exchange concerning visas issued by the Member States. The conflation of immigration and terrorism was apparent; in the Council’s own words, ‘[t]he events of 11 September 2001 […] radically altered the situation, showing that visas are not just about controlling immigration but are above all an issue of EU Member States' internal security.’ After the first shockwave, the Spanish delegation drew up a policy questionnaire envisaging a multi-purpose system that would store data on all visa applications irrespective of the decision reached in each case. In its meeting in Laeken in December 2001, the European Council called for the setting up of a common visa identification system, and in the following months the VIS featured prominently in the discussions as an instrument to contribute in the fight against irregular migration, or as an identification tool for return purposes. By June 2002, the establishment of the VIS was considered a ‘top priority’ and the JHA Council had approved a set of guidelines on its main features, which included the recording of biometric data and the use of the system for a multiplicity of purposes.

Preparatory work, including a feasibility study, continued until early 2004. In a rather confusing merging of immigration control and law enforcement imperatives, the JHA Council held in February 2004 that one of the purposes of the VIS would be to ‘contribute towards improving the administration of the common visa policy and towards internal security and combating terrorism’. Soon afterwards, the Commission

---

762 Baldaccini (n23) 32.
763 For previous efforts on establishing cooperation on visas see Brouwer (n17) 127.
767 European Council, Document DOC/1/18 (14/5.12.2001) pt 42.
768 See (n572).
772 Council, Document 9615/02 (05.06.2002). Also see Council, Documents 7309/02 (21.03.2002); 9243/02 (27.05.2002); 9615/02 (05.06.2002).
774 A rare reference to surveillance of external borders, which refers to the VIS as well, can be found in Commission, ‘Towards integrated border management of the external of Member States of the European Union’ (Communication) COM(2002) 233 final.
tabled a proposal for a Council Decision establishing the VIS,\textsuperscript{776} the adoption of which was accelerated by the Madrid bombings. Council Decision 2004/512/EC\textsuperscript{777} established the system in principle and authorised the Commission to begin the technical preparations for the set up of the VIS, whilst the political decision-making on the functions and content of the system was still in progress. The Decision thus formed the legal basis for the setting up of VIS in advance of a second, detailed legal instrument that would prescribe specific rules on its aims and functions. In December 2004, the Commission presented a proposal for a Regulation\textsuperscript{778} that was originally foreseen to be adopted in mid-2006 so that the system could begin its operations in 2007. On 24 February 2005, the JHA Council called for access to the VIS to be given to authorities responsible for internal security so that ‘the aim of enhancing internal security and counter-terrorism can […] be fully achieved’.\textsuperscript{779} Such access would be required ‘in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats’.\textsuperscript{780}

Since the core objective of the VIS would be the improvement of the EU common visa policy, the instrument had to be adopted by qualified majority voting, and through co-decision with the Parliament. Consultation of visa data for law enforcement purposes, however, fell within the remits of the former third pillar; hence a separate measure was necessary to be adopted under unanimity within the Council, with only the mere consultation of the Parliament. A proposal for a Council Decision aiming at regulating access by law enforcement authorities and Europol was released\textsuperscript{781} and both instruments were linked and negotiated in parallel. A first-reading agreement between the Council and the Parliament on the final text of the VIS Regulation\textsuperscript{782} was reached in June 2007, but the official adoption of the measure was considerably delayed until June 2008. The Decision was also formally adopted in 2008, legally based on Articles


\textsuperscript{777} See n729.


\textsuperscript{779} Council, Document 6228/05 (Presse 28, 04.03.2005) 15.

\textsuperscript{780} Council, Document 6811/05 (Presse 42, 14.03.2005); Also see Commission, ‘Improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs’ (Communication) COM(2005) 597 final, 6.

\textsuperscript{781} Commission, ‘Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences’ COM(2005) 600 final (Proposal for VIS Regulation).

\textsuperscript{782} For an overview of the negotiations see Council, Document 11632/06 (13.07.2006).
30(1)(b) and 34(2)(c) of Title IV TFEU. The two legal instruments were linked via a ‘bridging clause’.\textsuperscript{783}

3.2 VIS Regulation

3.2.1 Introduction to the VIS

The VIS Regulation requires national visa authorities to store in a centralised, database alphanumeric and biometric data on Schengen visa applicants and visas issued, revoked, annulled, extended or refused.\textsuperscript{784} Files on long-stay visas are not registered unless these are valid concurrently with a Schengen visa. A primary function of the VIS is to assist in the examination of visa applications. Whereas before the establishment of the VIS it had been possible for an applicant whose visa application had been rejected by one country’s consulate to continue applying to other consulates, the operation of the VIS means that this is no longer possible, as information on previous applications and reasons for rejection are available through the system.\textsuperscript{785} In this context, the VIS enables thorough and speedy background checks.

According to Article 48 of the VIS Regulation, the VIS would gradually become operational following a Commission Decision after the adoption of all the necessary implementing measures, having first completed a series of tests regarding its function, and after the Member States had notified the Commission that they are ready to transmit the necessary data from the first region in which the VIS was to become applicable.\textsuperscript{786} The decision on the first region would be decided through the comitology procedure on the basis of the following parameters: irregular migration, threats to internal security and the feasibility of collecting biometrics.\textsuperscript{787} In reality, Member States had already decided that the VIS would begin its operation in North Africa and the Middle East.\textsuperscript{788} Due to delays and technical complications,\textsuperscript{789} the phased ‘roll-out’ of the VIS,

\begin{itemize}
\item \textsuperscript{783} VIS Regulation, art 3.
\item \textsuperscript{784} ibid arts 10-14.
\item \textsuperscript{785} Baldaccini (n23) 40.
\item \textsuperscript{786} VIS Regulation, arts 48(1) and 51(2).
\item \textsuperscript{787} ibid art 48(4).
\item \textsuperscript{788} Council, Document 14390/05 (Presse 296, 01/02.12.2005).
\end{itemize}
comprising of 23 regions, commenced in November 2011 and was completed in
February 2016 with the inclusion of EU Schengen States.\footnote{Commission Implementing Decision (EU) 2016/281 of 26 February 2016 determining the date from which the Visa Information System (VIS) is to start its operations at external border crossing points [2016] OJ L52/64.}

The size and capabilities of the VIS are currently unrivalled in the EU, with the potential of storing up to 70 million fingerprints in the first five years of operation,\footnote{Commission, ‘Proposal for VIS Decision’ (n776) 4.} accessible by at least 12,000 users at 3,500 consular posts.\footnote{Council, Document 10267/07 (Presse 125, 25.06.2007).} In 2015, whilst the roll-out was still ongoing, the 26 Schengen States issued around 14.3 million Schengen visas. By the end of September 2015, the VIS was storing over 17 million registered visa applications, including 15.5 million data sets on Schengen visas issued. Notably at that time, regions 19 to 23 were still to be rolled out.\footnote{eu-LISA, ‘VIS Report pursuant to Article 50(3) of Regulation (EC) No 767/2008 - VIS Report pursuant to Article 17(3) of Council Decision 2008/633/JHA’ (2016) 16.} These data sets are currently available to all Schengen States, which have performed more than 254 million operations. Although Cyprus has expressed its interest in connecting to the system prior to becoming a full Schengen State, at the time of writing it is not yet connected to the system. The same applies for Romania, Bulgaria and Croatia.\footnote{ibid 11-12.} Since the VIS constitutes a development building upon the Schengen \textit{acquis}, the UK and Ireland do not take part either, although the former has challenged this exclusion in relation to the VIS Decision.\footnote{See below Section 3.2.2.}

Finally, synergies and interconnections between the VIS and the SIS were envisaged from the outset.\footnote{Commission, ‘Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)’ (Communication) COM(2003) 771 final.} However, these were not integrated in the final text. As with the SIS, the VIS is based on a centralised architecture comprising a central database (C-VIS) with alphanumerical searching capabilities and an Automated Fingerprint Identification System (AFIS) for fingerprint comparison, and an interface in each Member State constituting the national part of the system (N-VIS).\footnote{Council Decision establishing the VIS, art 1.}
3.2.2 The ‘umbrella’ purpose of the VIS and the case C-482/08 *UK v Council*

According to Article 2 of the Regulation, the VIS has the purpose of ‘improving the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States’. Under the auspices of this ‘umbrella’ purpose, no less than seven wide-ranging objectives are encompassed:

a) Facilitating the visa application procedure;
b) Preventing ‘visa shopping’;
c) Facilitating the fight against fraud;
d) Facilitating checks at external border crossing points and within national territory;
e) Assisting in the identification of persons that do not meet the requirements for entering, staying or residing in a Member State;
f) Facilitating the implementation of the Dublin mechanism for determining the Member State responsible for the examination of an asylum application and for examining such applications; and
g) Contributing to the prevention of threats to Member States’ internal security.\(^{798}\)

This rather confusing wording of Article 2, particularly the inclusion of the term ‘internal security’ that departs beyond the framework of visa policy, led to different views regarding the exact relationship and hierarchy among the different aims pursued. The EDPS claimed that the proposal identified the development of the common visa policy as the overarching objective of the VIS and set out a series of additional benefits, which did not constitute purposes on their own, but brought positive and welcome results to the setting up of the database, and the overall improvement of the common visa policy. He further categorised these benefits into primary and secondary ones, with the fight against visa shopping and fraud falling within the former category, and the facilitation of the Dublin system and the prevention of security threats falling within the latter category.\(^ {799}\) The divide between a purpose and a benefit was initially favoured by the Parliament,\(^ {800}\) but what the EDPS considered as primary benefits were promoted to objectives, whereas the secondary benefits were ‘baptised’ as ‘derived benefits’.

\(^{798}\) Compare with the proposal for a VIS Regulation (n776) where this aim was listed first.

\(^{799}\) An argument in favour of this classification stems from the wording of recital 5 of the VIS Regulation.

The legal ambiguity surrounding the ranking of VIS purposes has been resolved by the CJEU in *UK v Council*.\(^{801}\) Pursuant to its opt-out privileges, the UK did not form part of the negotiations for the adoption of the VIS Regulation, as this constitutes a development of the Schengen *acquis* to which it did not participate. In this context, the UK sought annulment of the VIS Decision on the grounds that it constitutes a police cooperation measure and, therefore, should have been given access to the VIS for law enforcement purposes. British law enforcement authorities could still have indirect access to visa data through Framework Decision 2006/960/JHA, governing information exchange in criminal law context,\(^{802}\) and Article 6 of the VIS Decision.\(^{803}\) Nevertheless, the UK took the view that although the VIS Regulation and Decision were complementary, still they were distinct from each other and must be assessed separately.\(^{804}\) In line with the Opinion of AG Mengozzi,\(^{805}\) the CJEU dismissed the UK arguments and upheld the VIS Decision, basing its reasoning on the effectiveness and the special nature of Schengen cooperation. Firstly, it noted that the need for coherence in the Schengen *acquis* must be taken into account,\(^{806}\) understood as meaning that the States taking part are not obliged during its development to take any adaptation measures.\(^{807}\) Although it contended that the aim of the VIS Decision falls within the sector of police cooperation, it opined that the content is related to both the common visa policy and police cooperation.\(^{808}\) Furthermore, the Court observed that:

> '[The VIS Decision] provisions nevertheless contain conditions restricting access to the VIS […] which make clear that they organise in essence the ancillary use of a database concerning visas, the principal purpose of which is linked to the control of borders and of entry to the territory and which is therefore available, merely by way of consultation, for police cooperation purposes on a secondary basis only, solely to the extent that use for those purposes does not call into question its principal use.'\(^{809}\)


\(^{803}\) See below, Section 3.3.

\(^{804}\) *UK v Council* (n801) ¶31-35.

\(^{805}\) Case C-482/08 *UK v Council* [2010] OJ I-10413, Opinion of AG Mengozzi.

\(^{806}\) *UK v Council* (n801) ¶48.

\(^{807}\) ibid ¶49.

\(^{808}\) ibid ¶50-51.

\(^{809}\) ibid ¶52.
Moreover, the Court found that the VIS Decision is closely linked to the VIS Regulation from both a functional and a practical point of view; the Decision could not exist independently of the VIS.\footnote{ibid ¶54.} In order to justify this statement, the Court mentioned that the UK did not have the technical infrastructure to have access to the system.\footnote{ibid ¶56.} In addition, if it were to accept the UK reasoning, this would lead to paradoxical situations whereby Member States that had not taken part in the negotiations for the establishment of the database would be able to consult it, whilst Schengen States that are not EU Member States would not.\footnote{ibid ¶58.}

The judgment clarified that the development of the common visa policy is the core objective and use of the database in law enforcement context has to be treated as secondary and collateral. In order to justify this view, the Court took note of the specific conditions of law enforcement access that testify for its exceptional character. It further highlighted that VIS data may be merely consulted for criminal law purposes, hence, arguably, excluding elaborate searches. Thus, opening up the VIS to criminal law agencies and Europol is an add-on, which is, by default, beyond the original purpose of the database, and that is why it is necessary to specify the rules and procedures of access in a limited manner. This corresponds to what the AG mentioned in his Opinion; that the VIS itself does not have a function linked to the prevention and punishment of crimes, thus the specific access should be treated as exceptional and limited.\footnote{UK v Council, Opinion of AG (n805) ¶10.} The finding that law enforcement access is not inherent in the VIS is important, particularly since the Commission, earlier that year, contended that ‘the original purpose of VIS was to facilitate the cross-border exchange of visa data, but this was later extended to preventing and combating terrorism and serious crime’.\footnote{Commission, ‘Overview of information management’ (n670) 22.} Another significant proclamation was that the VIS Decision remains closely linked to the parent VIS Regulation and is driven by its motivation and general objective. Therefore, when assessing the aim pursued, one cannot focus solely on the VIS Decision, but must take into account the VIS Regulation as well.

### 3.2.2 Categories of data

The VIS contains data that are gathered for five categories of visas: ‘short-stay’, ‘transit’, ‘airport transit’ of a limited territorial validity, and long-stay visas valid
concurrently as short-stay visas. A ‘touring visa’ is currently being negotiated and, if adopted, shall be included within the scope of the VIS as well. In particular, each visa authority is under the obligation to produce a digital application file based upon the visa application that includes the set of data mentioned in Articles 8 and 9 of the VIS Regulation, and check whether the applicant has been previously registered elsewhere. If so, a link to a previous application is created. Furthermore, links among separate applications are created if an applicant is travelling in a group or with their spouse and/or children.

According to Article 9 of the VIS Regulation, upon lodging a visa application, the following data from the application form must be recorded in the system:

a) Application number;

b) Information on the status of the application;

c) Authority with which the application has been lodged;

d) Names, sex, and place, date and country of birth;

e) Current nationality and nationality at birth;

f) Information concerning the travel document;

g) Place and date of the application;

h) Type of visa requested;

i) Details of the persons issuing an invitation and/or liable to pay the applicant’s subsistence costs during the stay, namely: a) in the case of a natural person, the name and address of the person, or b) in the case of a company or other organisation, the name and address of the company and the nationality of the contact person within that company/organisation;

j) Main destination and duration of the intended stay;

k) Purpose of travel (tourism, business, visit friends/family, cultural, sports, official reasons, medical visit, study, transit, airport transit, other);

l) Intended date of arrival and departure;

m) Intended border of first entry or transit route;

n) Residence;

o) Current occupation and employer and, for students, name of school;

p) Parents’ names (for minors);

q) Photograph; and

---

815 VIS Regulation, art 4(1).
817 VIS Regulation, art 8(2).
818 ibid art 8(3).
819 ibid art 8(4).
r) Full set of fingerprints. In accordance with the Common Consular Instructions, fingerprinting is compulsory for visa applicants over the age of 12.

Comparing to the information recorded in the visa application form, there are few categories of data that are not electronically recorded; the marital status, national identity number (where applicable), costs for travel and the additional information on family members who are EU/Schengen nationals. Furthermore, depending on the decision or procedure on the visa application, additional data are stored concerning the status of the visa, the issuing authority and the type of the visa. In particular, where a visa is refused, annulled, revoked or extended, the visa authority must state the reasons for such decisions.

The VIS is another example in EU law of the routine collection and further processing of biometric data on a massive scale in a process whereby the human body is tagged so that its movements through space can be recorded. Whereas the inclusion of a photograph in the application file was already envisaged in Regulation 1683/95, fingerprinting is a new element introduced to ‘ensure reliable verification and identification of visa applicants’. This means that when the applicant would be subject to checks post-registration, the comparison of fingerprints would confirm that the persons demonstrating the visa is indeed the person to whom the visa was initially issued (one-to-one search) and that in absence of documentary evidence, or use of falsified documents, a comparison of fingerprints with those stored in the VIS would identify the person (one-to-many searches). If, however, fingerprints cannot be registered, this fact must be indicated in the system, where it must be distinguished whether non-registration of fingerprint data is owing to legal (e.g. the person is below the age of 12) or factual reasons (e.g. destroyed fingerprints).

The ‘banality’ of biometric data is all the more evident in the Communication of April 2016 on stronger

---

820 Articles 6 and 7 of the proposal for VIS Regulation distinguished between data to be entered in all cases and a longer list of data to be entered in cases when a Member States is obliged to consult another’s authorities before making a decision on the application (consultation cases). Eventually this list was merged. See Council, Document 13861/06 (12.10.2006).
822 Compare with Visa Code (n754) annex 1.
823 Vis Regulation, arts 10-14.
824 ibid arts 12(2), 13(2), 14(2).
827 VIS Regulation, recital 10.
828 Council, Document 8198/07 (02.04.2007).
and smarter information systems for borders and security, where the Commission stated that the age limit for collecting fingerprints will be reduced to the age of 6.\footnote{Commission, ‘Stronger and Smarter Information Systems’ (n585) 9.} This rather controversial idea has been on the agenda for a decade,\footnote{This was advocated by the Council when negotiating a revision to the Common Consular Instructions in 2006. Council, Document 13610/06 (13.10.2006).} but until now has not been possible to incorporate for technical reasons.\footnote{For a study claiming that fingerprinting of children is technically feasible see Commission, ‘Fingerprinting recognition for children’ (JRC 2013).}

An addition proposed by the Council involved the possibility of registering data concerning the ‘misuse of a visa’.\footnote{Council, Document 9083/06 (08.05.2006) 5.} Such situations would arise in cases where the visa holder had stayed on the territory of a Member State ‘without authorisation […] following expiry of the visa’, had ‘unlawfully taken up employment’, or on the basis of other circumstances ‘which would have justified refusal of a visa or if a person’s liability to pay the costs of living during the stay […] was not complied with’.\footnote{Council, Document 11632/06 (n782) art 11a. For the objections to this proposal see Council, Document 9130/06 (08.05.2006).} On the basis of that additional facet of the VIS, the Council wished to extend the information stored on sponsors and persons inviting visa holders to include the sex and place and date of birth. However, that proposal was eventually blocked by the Parliament.\footnote{Council, Documents 11632/06 (n782); 13861/06 (n820).}

### 3.2.3 Retention period

The general retention period for data stored in the VIS is five years from a specified date;\footnote{VIS Regulation, art 25.} a) the expiration of the visa, if one has been issued and/or extended, b) the date of the creation of the application file in the VIS, in case an application has been withdrawn, closed or discontinued, or c) the date of the decision of the visa authority, if a visa has been refused, annulled or revoked. This essentially means that the minimum retention period is five years, but in the majority of applications that are successful, data are stored for longer depending on the duration of the validity of the visa. Furthermore, if a visa holder travels regularly to the EU, the storage period may essentially be renewed indefinitely. Only in cases when the visa applicant acquires the nationality of a Member State, or a refusal of issuing a visa is overturned, shall the data be deleted before their ‘expiration date’.\footnote{VIS Regulation, art 23. The Parliament had requested shorter retention period, but this suggestion was not followed. Parliament, ‘Draft Report on VIS Regulation’ (n800) 41-2.}
3.2.4 Accessing authorities

The diverging purposes for which the VIS is used reflects on the broad circle of accessing authorities. In particular, access to the VIS for entering, amending or deleting data is reserved exclusively to the duly authorised staff of national visa authorities,\footnote{ibid arts 6(1) and 6(3).} which are defined as those responsible for ‘examining and for taking decisions on visa applications or for decisions whether to annul, revoke or extend visas, including the central visa authorities and the authorities responsible for issuing visas at the border’.\footnote{ibid art 4(3).}

Furthermore, access for consultation is open to a wide range of authorities as long as ‘the data are required for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued’.\footnote{ibid art 6(2).} Once the information is entered, the VIS is used when examining visa applications.\footnote{ibid art 15(1).} Access is initially given to search specific categories of data, including fingerprints,\footnote{ibid art 15(2).} and in case of a ‘hit’, the entire application file and all linked files may be examined.\footnote{ibid art 15(3).} Another use of the VIS by visa authorities involves the consultation of other Member States’ authorities on whether to issue a visa and document exchange.\footnote{ibid art 16.}

Moreover, the VIS is accessed by external border control authorities via the visa sticker number and fingerprints, to authenticate the visa, verify the identity of the visa holder (one-to-one searches) and confirm that the conditions of entry are satisfied.\footnote{ibid art 18(1).} The possibility of using fingerprints to conduct searches at the external borders was the subject of a debate with the Parliament rejecting \textit{prima facie} such functionality claiming that this would excessively disturb border crossing.\footnote{For the discussions see Council, Documents 5213/07 (11.01.2007) 36-7; 8185/07 (12.04.2007) 3; 8540/07 (18.04.2007) 2.} As a compromise, the VIS Regulation introduces a flexible transitional period of three years during which searches on the basis of fingerprints do not take place.\footnote{VIS Regulation, art 18(2).} The obligation to consult the VIS upon entry was inserted through an amendment to Regulation 526/2006,\footnote{Regulation (EC) 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code [2009] OJ L35/56.} including the three-year derogation, which have started three years after the beginning of VIS
operations. Furthermore, Article 8 of Regulation 2016/399\(^{848}\) – which is the latest version of the Schengen Borders Code (SBC)– states that the VIS must be consulted upon both entry and exit. Consultations occur using the number of the visa sticker in all cases and, on a random basis, the visa sticker is combined with a verification of fingerprints when intense traffic results in excessive delays at border crossing points, when all resources have been exhausted as regards to staff, facilities and organization, and on the basis of an assessment that there are no risks related to internal security and illegal immigration.

In addition, immigration authorities may have access to VIS data within national territories in order to verify the identity of a person, check the authenticity of the visa, or confirm that they fulfill the conditions for entry, stay or residence. In order to identify a person (one-to-many searches) who may be an irregular migrant, national immigration authorities or border guards may conduct searches in the VIS using fingerprints.\(^{849}\) Asylum authorities may enter the fingerprints of an asylum seeker for comparison for Dublin-related purposes, or for the purpose of examining the merits of an asylum claim.\(^{850}\)

The Regulation stipulates that each Member State must communicate to the Commission a list of the competent authorities whose staff are authorised to enter, amend, delete or consult data in the VIS, along with the details of the central authority designated as responsible for the processing of that data. The Commission annually publishes an updated, consolidated list of these authorities where amendments have been made.\(^{851}\)

### 3.2.5 Transfer of data

Communication of data to third countries or international organisations\(^{852}\) is prohibited,\(^{853}\) except if necessary in individual cases to attest a third-country national’s

---


\(^{849}\) ibid art 20.

\(^{850}\) See Chapter 4. For an overview see Council, Document 6747/15 (03.05.2015).

\(^{851}\) VIS Regulation, art 5. For the latest list see Notices from Member States, ‘List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS)’ [2016] OJ C187/4.

\(^{852}\) Such as the UN organisations, IOM and Red Cross.

\(^{853}\) Peers rightly notes that the situation is unclear with regard to non-Schengen EU Member States. Steve Peers, ‘Legislative Update: EC Immigration and Asylum Law 2008: Visa Information System’ (2009) 11 European Journal of Migration and Law 69, 87-8. This provision was not included in the proposal, but was introduced by the Council. See Council, Document 18617/06 (20.12.2006) 52. The
identity for the purpose of their return. Such transfer is possible only if a series of conditions are cumulatively met: a) an adequacy Commission decision regarding the level of data protection in the third country, or if Article 26(1)(d) of the Data Protection Directive applies, or a readmission agreement between the EU and that third country exists; b) the third country, or international organisation, agrees to use the data solely for the purpose of return; c) the data transferred must be in compliance with the relevant EU data protection provisions; and d) the Member State that entered the data must have provided their consent. The VIS Regulation further prescribes that such transfers ‘shall not prejudice the rights of refugees and persons requesting international protection, in particular as regards non-refoulement’, but it is unclear how this principle is observed in cases when data are transferred. As for the data that may be transferred, these are: names, nationality, residence, travel documents and (for minors) parents’ names. In effect, photographs, fingerprints and other alphanumeric data are excluded.

3.2.6 Individual rights

Article 37 sets out individual rights, which are comparable to those prescribed in the SIS II Regulation. As two authors have observed, the VIS Regulation provides a higher level of protection. As regards the right of information, visa applicants and sponsors must be informed of the identity and contact details of the controller, the purposes for which the data are processed within the VIS, the categories of the recipients of the data, the retention period of the data, the mandatory character of their collection and the right to access and to correct and delete the data, including information on the procedures to exercise such rights. In relation to the right of access, the Regulation stipulates that any person must be entitled to obtain communication of the data relating to them recorded in the VIS and of the Member State that stored them in the system, and request that inaccurate data relating to him/her be corrected, or that
unlawfully recorded data be deleted. Individuals concerned may bring an action before the competent courts of that Member State if they are refused the right of access to, or the right of correction or deletion of, data relating to them.

3.2.7 Supervision

As in the case of the SIS II, supervisory tasks are shared between national DPAs and the EDPS. The former enjoy the rights envisaged in the Data Protection Directive and monitor the lawfulness of the processing of personal data by Member States, whereas the latter is entrusted with monitoring the activities of eu-LISA. The EDPS and the national supervisory authorities are to cooperate actively, in particular to coordinate the management of the VIS and the national interfaces.

3.2.8 ‘Bridging’ clause

Article 3 of the VIS Regulation constitutes the ‘bridging’ clause linking the Regulation to the parallel third pillar Decision governing consultation of the VIS by law enforcement authorities and Europol. This intensely negotiated provision that was not envisaged in the proposal stipulates the core rules on law enforcement access in an attempt by the Parliament to ‘squeeze’ in as many safeguards as possible, given that the adoption of the VIS Decision was not under its direct negotiating influence.

According to Article 3(1), national ‘designated’ authorities may access VIS data in individual cases following a reasoned written or electronic request ‘if there are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection and investigation of terrorist offences and of

---

862 ibid art 38(2).
863 ibid art 40.
864 ibid art 41.
865 ibid art 42.
866 In this respect, a VIS Supervision Coordination Group has been set up. Its first report on the period 2012-2014 can be found in Council, Document 14365/15 (25.11.2015).
867 In an informal discussion with an Official from the Parliament, it was highlighted that literally every word contained in the bridging clause was rigorously negotiated (Brussels, November 2014).
868 As Peers notes, the decision to grant law enforcement access to VIS data was taken after the proposal had been tabled. The proposal included the prevention of internal threats among the objectives. See Steve Peers, ‘Legislative Update: Visa Information System’ (n853) 75.
869 The Parliament Rapporteur wished the negotiation of the measures as a package in order to circumvent the consultation procedure. Council, Document 9753/07 (19.06.2007) 3.
other serious criminal offences’. Europol may also access the system ‘within the limits of its mandate and when necessary for the performance of its tasks’. Furthermore, access can be obtained through central access points, which will act as verifying authorities checking whether the conditions for access have been met. ‘Member States may designate more than one central access point to reflect their organisational and administrative structure’. In urgent cases, verification could take place ex post. Transfers of data to third countries or international organisations are prohibited unless there is an exceptional case of urgency involving the prevention and detection of terrorist offences and other serious crimes. In such cases, records of transfers must be kept and made available to DPAs. The Regulation is also ‘without prejudice’ to the obligation under national law for visa authorities to inform domestic police or prosecutorial authorities about suspected criminal acts.

Overall, the Parliament succeeded in two main respects. Firstly, it secured that the central access point, which would check the request for access before a search could take place, would come from a different unit, even within the same national authority, in exchange that access without prior verification could take place in urgent cases, and that Member States could designate more than one such unit. Secondly, it secured that the VIS Decision would include a series of data protection provisions.

3.3 VIS Decision

As seen above, the prevention of EU internal security threats has been regarded by Member States as a ‘window of opportunity’ to introduce an additional functionality into the VIS. This expansion is in line with the broader context of the legal environment formulated post-9/11, whereby emphasis is placed on preventive justice as a means to

---

870 The Parliament had a list of four conditions for law enforcement access, whereas the Council wanted only a brief reference in this respect. See Council, Document 11632/06 (n782); Parliament, ‘Draft Report on VIS Regulation’ (n800). However, the Council doubted as to whether that wording would permit the effective prevention, detection and investigation of terrorist acts or other serious crimes. Also see Council, Document 15271/05 (01.12.2005).
871 VIS Regulation, art 3(1).
872 ibid art 3(2).
873 ibid.
874 The Parliament wished to exclude transfers completely. Council, Document 11632/06 (n782).
875 VIS Regulation, art 3(4).
876 The Parliament also succeeded in changing the wording from ‘a serious and imminent threat’ to the higher threshold of ‘an exceptional case of urgency’. Peers, ‘Legislative Update: Visa Information System’ (n853) 75.
877 ibid.
878 For the negotiations see Council Documents 8185/07 (n845); 8540/07 (n845) and 9128/07 (02.05.2007).
pre-empt future acts which are considered as security threats. The preventive model is grounded on the construction of suspect individuals on the basis of a constant risk assessment. The VIS, which stores data of individuals whose countries of origin have already been profiled as risky, provided the ideal environment for an exploitation of the data collected, leading to a controversial ‘cross-fertilisation’ and convergence between border controls and criminal law. Therefore, whereas the VIS Regulation aimed at preventing entry within the context of immigration control, the VIS Decision extended prevention in the criminal law framework, leading to an indirect criminalisation and securitisation of migration control.

Against this background, the VIS Decision circumscribes the modalities of access by police authorities and Europol. Such access is granted solely for the purposes of the prevention, detection and investigation of terrorist offences and other serious crimes. According to Article 2 of the VIS Decision, terrorist offences correspond, or are equivalent, to those referred to in Articles 1-4 of Framework Decision 2002/475/JHA on combating terrorism, as amended by Framework Decision 2008/919/JHA. Serious crimes are specified in Article 2(2) of Framework Decision 2002/584/JHA on the EAW. The VIS Decision became effective on 1 September 2013, pursuant to Council Decision 2013/392/EU, which was annulled by the CJEU on the grounds that the Parliament had not been consulted prior to its adoption. The Court decided to maintain the legal effects of the Decision until the entry into force of a replacement act. Following the judgment, Council Decision 2015/1956 was adopted, this time in

880 Valsamis Mitsilegas, EU Criminal Law after Lisbon (n688) ch 9.
881 VIS Decision, art 8(3).
884 See n596.
consultation with the Parliament. As for Europol, to the best of my knowledge, the Agency is not yet connected to the VIS.\(^{888}\)

### 3.3.1 Authorities

Access to the VIS is granted to national ‘designated’ authorities defined as those ‘responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences’.\(^{889}\) The term ‘designated authorities’ was a later addition to the Decision, as the Commission envisaged access to the VIS to be given to ‘authorities responsible for internal security’,\(^{890}\) also understood under the aforementioned definition.\(^ {891}\) However, this wording left open the question as to whether security services were covered, leading several Member States to request an amendment and a verbatim exclusion of such authorities from the new definition.\(^ {892}\) Whereas a replacement term was indeed favoured in the final text,\(^ {893}\) there is no prohibition of allowing security agencies to process the VIS data.\(^ {894}\)

According to Article 3(2) of the VIS Decision, a list of the designated authorities and the central access point(s) must be communicated to the Commission and the General Secretariat of the Council. The Commission has published such lists in the *Official Journal of the EU*.\(^ {895}\) Furthermore, at national level, each Member State must keep a list of the operating units within the designated authorities that are authorised to access the VIS.\(^ {896}\) The Decision states that access must only be granted to those who ‘have a need to know’ and have knowledge on data security and data protection.\(^ {897}\) Europol must also designate a specialised unit to act as a central access point.\(^ {898}\)

\(^{888}\) eu-LISA, ‘VIS Report’ (n793) 23.  
\(^{889}\) VIS Decision, art 2(1)(e).  
\(^{890}\) Commission, ‘Proposal for VIS Decision’ (n776) art 2(e).  
\(^{891}\) Council, Document 9199/06 (11.05.2006) 2.  
\(^{892}\) ibid.  
\(^{893}\) Council, Document 5456/1/07 (20.02.2007). Also see Council, Document 14196/06 (23.11.2006).  
\(^{894}\) Brouwer (n17) 132.  
\(^{895}\) Notices from Member States, ‘Declarations concerning Member States’ designated authorities and central access point(s) for access to Visa Information System data for consultation in accordance with Article 3(2) and 3(3) respectively of Council Decision 2008/633/JHA’ [2013] OJ C236/1.  
\(^{896}\) VIS Decision, art 3(5). Member States preferred a system of declarations as opposed to a comitology procedure. Council, Document 5199/06 (12.01.2006) 2.  
\(^{897}\) VIS Decision, Recital 6.  
\(^{898}\) ibid art 7(3).
3.3.2 Procedure

If a national operating unit wishes to consult the VIS, it must submit a reasoned written or electronic request to the central access point.\textsuperscript{899} The latter must then verify that the requirements for access, as outlined below, are met and, if so, the request is processed accordingly.\textsuperscript{900} Derogation from this procedure is foreseen solely in exceptional cases of urgency, whereby the requests are processed immediately and verification of the conditions of access takes place ex post.

According to Article 5(2) of the VIS Decision, any of the following categories of data may be used as search keys: names; sex; date, place and country of birth; nationality; travel document; main destination and duration of intended stay; purpose of travel; intended date of arrival and departure; intended border of first entry or transit route; residence; fingerprints; visa information and details of the persons issuing an invitation or sponsoring the stay. Data from the application form, photographs\textsuperscript{901} and any data subsequently entered will show up in the event of a ‘hit’,\textsuperscript{902} however the Regulation is unclear as to whether links with other applications will also show.

3.3.3 Conditions

As an ancillary purpose of the VIS, access to national law enforcement authorities is subject to three specific conditions.\textsuperscript{903} Firstly, access must be necessary for the prevention, detection or investigation of terrorist offences or other serious criminal acts. Secondly, access must involve a specific case, meaning that the processing is allowed on a case-by-case basis and routine access is precluded.\textsuperscript{904} A specific case exists in particular:

\textsuperscript{899} ibid art 4. It must be noted that Member States opposed this procedure and wished direct access. Council, Document 9641/06 (07.06.2006) 4.

\textsuperscript{900} Initially a large number of Member States were opposed to this claiming operational reasons. See Council, Document 9199/06 (n891) 3.

\textsuperscript{901} Compare with the proposal for VIS Decision, where photographs were included in the list of search keys. The EDPS expressed concerns in this respect. EDPS, ‘Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final)’ [2006] OJ C97/6, 8.

\textsuperscript{902} VIS Decision, art 5(3).

\textsuperscript{903} ibid art 5(1). Furthermore, according to Article 6 of the VIS Decision, Member States which are not yet connected to the VIS may access the system, subject to same conditions and following the transmission of a request to a Member State in which the VIS is operational.

\textsuperscript{904} ibid recital 8.
'when the access for consultation is connected to a specific event or to danger associated with serious crime, or to (a) specific person(s) in respect of whom there are serious grounds of believing that the person(s) will commit or has (have) committed terrorist offences or other serious criminal offences or that the person(s) has (have) a relevant connection with such (a) person(s).'

Thirdly, there must be reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. The proposal referred to the higher threshold of ‘factual indications’ as forming the basis of reasonable grounds. However, this view was abandoned, with the Council stating that such a requirement would de facto make it impossible to access the system for preventing terrorist offences.

Europol may consult the VIS ‘within the limits of its mandate’ and when necessary for the performance of its tasks. Article 7(1) of the VIS Decision refers to the use of visa data in analysis work files and distinction is made between specific analyses on the one hand, and analysis of a general nature and of a strategic type on the other. In the latter cases, the VIS data must be rendered anonymous prior to the processing and only be retained in a form that excludes the identification of the data subject.

### 3.3.4 Transfer of data

Article 8(4) of the VIS Decision stipulates that personal data obtained from the VIS must not be transferred or made available to a third country or an international organisation. However, in an exceptional case of urgency, such data may be transferred or made available to a third country or an international organisation ‘exclusively for the purposes of the prevention and detection of terrorist offences and of other serious criminal offences’, subject to the consent of the Member State that entered the data into the VIS, and in accordance with the national law of the Member State transferring the data or making them available.

---

905 Emphasis added. The addition of the word ‘substantially’ was suggested by the EDPS. EDPS, ‘Opinion on the proposal for VIS Decision’ (n901) 3.
906 Council, Documents 11405/06 (03.08.2006) 8; 9083/06 (n832).
907 Council, Document 5456/1/07 (n893) 2.
908 The main task of Europol is to support cooperation between law enforcement authorities across Member States by processing, analysing and exchanging data either provided by Member States or produced by the Agency itself. For the legislative framework of Europol see n100. For an analysis see Mitsilegas, EU Criminal Law (n458) 161ff.
909 VIS Decision, art 7.
4. Evaluation of the VIS in light of Article 7 EUCFR

4.1 Application of Article 7 EUCFR

The VIS legal framework requires the collection and storage of a series of personal information on visa applicants, and persons linked to their visit to the EU, for various objectives spanning from visa policy-related ones to the prevention, detection or investigation of terrorist offences or other serious crimes. In particular, pursuant to Articles 9-14 of the VIS Regulation, the VIS stores alphanumeric information on the visa applicant regarding their nationality (including any previous nationality), information on persons who may have issued an invitation to them or are sponsoring their stay, information on their planned stay in the Schengen area (such as the dates and destination, residence, occupation), and two types of biometric data. These extensive categories of personal data are updated depending on the outcome of the decision and may be complemented with links to other VIS records or persons associated with them, such as family members.

Although Digital Rights Ireland scrutinises the retention of telecommunications data, which are somewhat different from the types of information set out above, in my view, the Data Retention Directive and the VIS framework share similar characteristics regarding the nature of the interference and the effects on the individual. Taken as a whole, the VIS data reveal a wealth of information concerning the private lives of visa applicants, such as their place of residence and their movements in the EU over a significant period of time, including the timings and choices of destinations. Personal habits or medical conditions may be indicated via the registration of the purpose of travel, which could include culture, sports or medical reasons. Furthermore, it is recalled that the ECtHR has held that the protection of Article 8 ECHR is not limited to the private sphere or the home of the individual, but includes ‘the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional and business nature’. In this respect, the VIS allows for drawing precise conclusions on professional activities pursued by visa applicants not only in their country of residence, but also in the EU, particularly since the purpose of travel must be indicated. Further conclusions may be drawn in cases when companies or organisations issue invitations or sponsor their stays. Information on this latter point may, in general, reveal personal and social relationships with other persons who may be EU or non-EU nationals. Links between applications are liable to reveal further social

910 Niemietz v Germany (n181) ¶29.
relationships of those people, as well as family ties. Visa applicants cannot be considered as consenting to the processing of their personal data, since it is mandatory for the nationals of certain countries to obtain a visa to enter the Schengen territory. Therefore, if they wish (or have a need) to travel to the EU they must subject themselves to the visa application procedure as set out in the relevant EU legal instruments.

The VIS is thus ‘showcased’ as a powerful tool enabling national authorities to construct a complete profile of visa applicants’ private lives. A significant portion of a person’s conduct is mapped and traced, to which a certain identity is attached through the inclusion of a photograph and fingerprints, which are also considered as forming part of a person’s private life. The build-up of this profile takes place through the registration of everyday information and is triggered solely by the pursuit of, what is in principle, perfectly legitimate activities, such as travelling or sponsoring a visa applicant.\textsuperscript{911} In this context, the collection and storage of visa data directly affects private life and consequently constitutes in itself an interference with Article 7 EUCFR. Access and transfer of data to law enforcement authorities and Europol under the rules provided by the VIS Decision constitutes a further interference with privacy, as it enlarges the group of authorities to which information may be disclosed.\textsuperscript{912}

The interference caused by the VIS legal framework with the fundamental right to privacy must be considered wide-ranging and must also be regarded as particularly serious for three main reasons. Firstly, the magnitude of the VIS must not be forgotten.\textsuperscript{913} It currentlycatalogues profiles on around 17 million visa applicants, and has the potential to store up to 70 million files, each containing large amounts of contemporary and sensitive personal information created, stored and further processed. The storage allows examination in a plethora of loci, timings and contexts: from the initial examination of the visa application to background checks in subsequent applications; from extraterritorial control in the country of origin to internal checks within the EU territory; and from the original forum of visa policy within which it was originally designed to performance in criminal investigations. In this context, the collection of VIS data establishes the conditions of mass surveillance of movement, which may generate in the minds of individuals, including those persons to whom their application is linked, the vague feeling that they are being monitored not only during their intended stay, but, importantly, throughout the retention period. This surveillance is further exemplified by the fact that the VIS essentially allows visa authorities to

\textsuperscript{911} Mitsilegas, \textit{EU Criminal Law} (n458) 249.
\textsuperscript{912} Weber and Saravia v Germany (n260) ¶79
\textsuperscript{913} By analogy to Digital Rights Ireland (n326) ¶37.
perform thorough background checks on individuals when examining their visa applications, or when performing checks on them. The establishment of the VIS entails that the mere choice, or need, to enter the EU territory equates with ‘stripping off’ their privacy through the disclosure and storage of a broad range of personal data. This process involves individuals against whom national authorities do not have negative associations and who, in principle, do not ‘belong territorially’ to the EU (and in their vast majority do not wish to do so), but for whom their liaison with the EU is only temporary. The fact that this information may end up at the hands of law enforcement authorities and Europol accentuates the feeling of surveillance and exemplifies the suspicion surrounding visa applicants as a group of ‘risky’ individuals who must be surveyed for both immigration control and criminal law purposes. It disregards the fact that the vast majority of visa applicants have lawful documents and legitimate grounds for traveling. Secondly, as in the case of the SIS II, the interference involves the collection and further processing of sensitive personal data. The fact that both types of biometric data are processed deepens the feeling of surveillance, particularly since the fingerprinting is connotated with criminality. Thirdly, it must be recalled that the operation of the VIS necessarily involves end-users (accessing authorities) in different consulates worldwide that are situated outside the EU. Furthermore, private service providers may be co-opted in the visa application process. Both factors significantly enhance the risks of abuse.

**4.2 Essence of privacy**

As noted in Chapter 2, in light of the sensitive nature of biometric data and the stigmatising effect of treating visa applicants as persons suspected of irregular migration or criminality, particularly since their personal data are stored for a significant period of time, it is arguable that generalised and indiscriminate collection and further processing of biometric data in massive databases goes to the core of privacy protection, particularly when this information is used in a multiplicity of contexts and involves *a priori* innocent individuals. The case of the VIS is such an example, whereby two categories of sensitive data (fingerprints and photographs) are collected and processed *en masse* and in relation to a plethora of State activities.

---

914 See Chapter 2, Section 5.4.
4.3 Objective of general interest

The VIS has been conceptualised from the outset as a multi-purpose tool under the overarching aim of implementing the EU common visa policy. Within the remits of this aim a series of sub-purposes are included, such as prevention of identity fraud, administration of visa policy, assisting identification of irregular migrants, assisting in the implementation of the common asylum policy, and the prevention of internal threats in the EU. In *Schwarz*, the CJEU recognised the fight against identity theft and irregular migration as constituting objectives of general interest,\(^915\) whereas in *Digital Rights Ireland* it found the fight against terrorism and other serious crimes as of utmost importance.\(^916\) Therefore, the VIS must be considered as pursuing objectives of general interest.

4.4 Is the limitation ‘provided for by law’?

According to the case law of the ECtHR, that expression requires, in essence, that the measure in question is accessible and sufficiently foreseeable, meaning that it provides adequate indication as to the circumstances in which, and conditions on which, it allows the authorities to resort to measures affecting their privacy. Whereas the ‘accessibility’ criterion is satisfied through the publication in the *Official Journal of the EU*, the ‘foreseeability’ criterion entails an examination of the quality of the law. Overall, both the legal instruments in question are drafted in sufficiently clear terms enabling visa applicants to understand, at least to an acceptable extent, the conditions for collecting, storing, processing and transferring of their data within the VIS framework. The rules on access and use of data by national authorities are rather comprehensive, the individual rights are set out in detail, and rules on data security are foreseen.

Nevertheless, whereas it is recognised that the typical elements for satisfying this criterion are met, law enforcement access to VIS data is at odds with the overarching aim of the development of the common visa policy. It is true that visa data may be, in certain cases, useful in the identification of perpetrators of terrorism or any other criminal offence, as may information on any other individual, be they an EU national or third-country national. The fact that Article 2 of the VIS Regulation refers to the ‘prevention of internal security threats’ does not necessarily mean that the data should

\(^{915}\) *Schwarz* (n320) ¶36-8.

\(^{916}\) *Digital Rights Ireland* (n326) ¶41-4.
be consulted during criminal investigations. Rather, it should have been seen as the additional benefit deriving from the VIS that, in cases where the examination of a visa application or the performance of checks would reveal that certain individuals are risky for the internal security of the EU, lead to those people not being granted a visa or not being admitted into the Schengen area. The inclusion of that purpose in the VIS Regulation acted as the ‘Trojan horse’ paving the way for subsequent extension of the VIS functionalities in the criminal law framework, but this ancillary objective, *in abstracto*, is beyond what an average individual would foresee when applying for their visa. As such, it constitutes an attack on the purpose limitation principle of data protection law, a strong disregard of the specificity of the purpose of the collection of the data, which is an immigration control,\(^{917}\) leading to blurring of the boundaries between that and policing.

### 4.5 Proportionality of the VIS as an immigration and asylum tool

In assessing the proportionality of the VIS as a management instrument supporting the EU common visa policy, it is useful to recall that in *Digital Rights Ireland* the Grand Chamber found that:

> ‘the extent of the EU’s legislature may prove to be limited, depending on a number of factors, including, in particular the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference’.\(^{918}\)

In this judgment, the Court placed significant limits to surveillance practices deployed on a massive scale as a means of contributing in the fight against terrorism and serious crime and, ultimately, to public security.\(^{919}\) The limitations were thus imposed in the most difficult context; that of law enforcement, which is of utmost importance, and its effectiveness is based largely on the gathering and exchange of personal data, which may lead to maximised surveillance. As it has been explained in Chapter 1, the discretionary power enjoyed by the legislature is relatively wide in view of the particularities of criminal investigations. By contrast, the main objective of the VIS is, in the CJEU’s own words, ‘linked to the control of borders and of entry to the territory’\(^{920}\) and, therefore, only indirectly related to the prevention of crime. Although the VIS improves the knowledge of the national immigration authorities on every visa

---

\(^{917}\) Mitsilegas, *The Criminalisation of Migration in Europe* (n8) 29, 43.

\(^{918}\) *Digital Rights Ireland* (n326) ¶47. See also Chapter 1, Section 4.3.3.

\(^{919}\) ibid ¶41-3.

\(^{920}\) *UK v Council* (n801) ¶52.
applicant and, despite its undisputed counter-terrorism origins, the CJEU has made clear that the nature of the VIS is administrative. Against this backdrop the threshold for privacy protection of individuals must be set even higher than in Digital Rights Ireland. The fact that law enforcement authorities and Europol may, under certain conditions, have access to visa data is irrelevant, as this is an ancillary objective which ‘must not call into question the primary objective’. Therefore, in the case of the VIS, the margin of discretion enjoyed by the EU legislator is significantly limited in view of three cumulative circumstances: the important role played by the protection of personal data in light of the fundamental right to respect for private life, the extent and seriousness of the interference with that right caused by the establishment and operation of the VIS, \(^\text{921}\) and the objective pursued.

**4.5.1 Personal scope**

Against this background, the VIS constitutes an exchange system of visa information, whereby all applicants that avail themselves of the VIS to grant any of the visas mentioned above must be registered in the system on a mandatory basis. In effect, all persons seeking access to an EU Member State subject to a visa requirement for their entrance are covered by the personal scope of the VIS. As such, the VIS Regulation requires the collection and further processing of visa data *en masse*. In effect, the VIS covers, in an indiscriminate manner, all visa applicants and all persons issuing invitations or sponsoring their stays, notwithstanding the fact that the majority of them have perfectly legitimate grounds to travel to the EU, or invite persons, ranging from professional activities, family ties, health reasons or student visits. As Peers observes, certain categories of third-country nationals who are family members of EU citizens and require a visa to enter the EU are not excluded. \(^\text{922}\) This involves either if they reside in a non-Schengen Member State and do not hold a residence card and they wish to enter the Schengen area, or if they are residing in a Schengen State but do not qualify for freedom to travel within the Schengen area, because they are not holders of a specified national residence permit or provisional residence permit. \(^\text{923}\) Furthermore, it is recalled that 15 million data sets stored in the system relate to third-country nationals who have been issued a visa, which means that they have successfully passed the risk assessment process. However, the collection and storage of personal information is mandated in all

\(^{921}\) By analogy to *Digital Rights Ireland* (n326) ¶48.

\(^{922}\) Peers, ‘Legislative Update: Visa Information System’ (n853) 77.

\(^{923}\) Ibid.
cases even though there may be no evidence of suggesting that their conduct may be linked to ‘visa shopping’ or attempted visa fraud, or that the person concerned may overstay their visa. Such evidence may only exist with reference to visas refused, annulled or revoked when the respective decision is based on the relevant substantial grounds (e.g. if the person has a counterfeit travel document or is considered to present a risk of irregular migration, or a SIS alert has been issued in their respect). In addition, information in relation to discontinued applications is also stored and may be processed and exchanged, irrespective of the reasons of that discontinuation, which may be purely coincidental or procedural. As such, the VIS constitutes a form of constant and semi-permanent risk assessment of visa holders, whereby the stigma of riskiness is never fully revoked.

4.5.2 Categories of alphanumeric data

For each individual file the VIS Regulation mandates the collection and storage of a variety of everyday personal data. As such, the existence of the system enables practices of profiling in the form of performing risk assessments of visa applicants when examining their applications. By focusing on pre-emption and the prediction of future behaviour, it provides officials and governments with extensive knowledge of every person who is seeking access to the EU, and paves the way of further categorising individuals in terms of their riskiness. Key in this respect is the listing of nationality as one of the search keys for examining visa applications, which may be used for establishing patterns of behaviour on the basis of the country of origin and examining travel routes. On the basis of VIS pre-emptive surveillance, visa applicants may thus be subject to discriminatory practices resulting in hindering of their freedom of movement, with significant consequences upon their private life. Furthermore, as Solove notes, such predictive determinations about one’s future behaviour are much more difficult to contest than investigative determinations about one’s past. Also questionable is the listing of the nationality at birth among the categories of data collected and possibly used as a search key, as it does not relate to the implementation of the common visa policy and may, in fact, give rise to prohibited discriminatory treatment between

924 VIS Regulation, arts 12(2)(b), (c), (f).
applicants that are nationals of the same third country.\textsuperscript{927} Even if such information is necessary in certain cases, it could be stored in the application file and made available upon request solely in the consultation procedure.\textsuperscript{928}

Another category of data that raises proportionality issues is that of persons issuing an invitation or sponsoring the stay of a person, who may be EU citizens or third-country long-term residents. Admittedly, the details of these persons or companies/organisations may be relevant, or even necessary, in relation to specific queries with regard to certain individuals and specific breaches of legal provisions.\textsuperscript{929} Therefore, their processing may be useful in cases of consultation between national visa authorities pursuant to Article 16 of the VIS Regulation. However, unless there is justified need, in the course of routine implementation of the visa policy the processing of these data is excessive and disproportionate. It could even amount to indirect discrimination, as lawful residents who are third-country nationals will invite their family members far more often than EU citizens. This is particularly the case since, according to Article 15(2)(d) of the Regulation, the details of natural or legal persons who issue an invitation or sponsor a visit may be used as search keys for examining applications without restrictions. The inclusion of these data seems to suggest the creation of a separate, informal mini-register on the side, whereby information of persons with connections to visa applicants of any kind – professional or personal – is collected and stored therein. The suspicion against visa applicants is, therefore, also extended to persons or organisations that are linked to them. This issue had actually been the subject of debate, with Member States wishing to extend the categories of data collected under the view that a Schengen-wide database would provide information on individuals inviting large numbers of visa applicants to several Member States.\textsuperscript{930} The functionality was directly linked to the possible use of the VIS for exploitation of data, an idea which, as mentioned above, was eventually abandoned.

The possible interlinking of application files allowed in relation to families or group members is another disproportionate feature of the VIS. In particular, the definition of this latter category as ‘obliged for legal reasons to enter and leave the territory of the Member States together’ lacks clarity and requires further explanation. Furthermore, it must not be forgotten that ‘the more different categories of data are

\textsuperscript{927} Article 29 DPWP, ‘Opinion 2/2005’ (n701) 11.
\textsuperscript{928} ibid.
\textsuperscript{929} ibid 15.
\textsuperscript{930} Council, Document 15271/05 (n870) 2.
entered into the VIS, the higher the risk that the information recorded is wrong, inaccurate or outdated”.  

4.5.3 Inclusion of biometric data

The collection and further processing of biometrics is a central aspect of the performance of the database. Legal challenges analysed in Chapter 2 regarding the reliability of biometric data, particularly when used for identification purposes, and their possible use in a manner unforeseen at the time of collection are relevant also in the present case, especially since a wide array of authorities are granted access. When the VIS Regulation was negotiated, the EDPS highlighted the limitations of fingerprinting. In particular, up to 5% of people are unable to enroll their fingerprints (FTE) either because they are not readable or because they do not have any fingerprints at all. He observed that in a system of 20 million applications, such as the VIS, this percentage amounts to up one million applicants who would not be able to follow the official registration process. Technology has since evolved, but the Technical Study on the development of forthcoming EES states that the FTE of the VIS remains around 5% due to a quality control and rejection mechanism. In practice, according to the latest report on the operation of the system until late 2013, over 25% of applications were without fingerprints, a rate that dropped to 20% of the total number of applications processed until late 2015. Furthermore, 36% of the registered applications without fingerprints did not contain that data due the fact that it was factually impossible for the applicant to provide fingerprints. In view of these divergent statistics that question the appropriateness and the effectiveness of the VIS, the mechanisms securing that only data of sufficient quality are entered into the system have been abolished, and all fingerprints enrolled may be stored and further processed at central level. Although the VIS Regulation includes a provision regarding the reasons why fingerprints have not been provided distinguishing between factual (e.g. not yet technologically feasible) and

932 See Chapter 2, Section 5.5.2.  
933 EDPS, ‘Opinion on the proposal for VIS Regulation’ (n352) 19.  
934 ibid.  
936 This number is affected by the fact that in certain Member States started operations before the official roll-out without capturing fingerprints. eu-LISA, ‘VIS Report’ (n793)18.  
937 ibid 18-19.  
938 ibid.  
939 eu-LISA, ‘VIS Report’ (n793) 10.
legal reasons (e.g. exemption due to age restrictions), it is reported that Member States are not always in compliance with these rules on how to indicate the reasons for not collecting fingerprints, affecting the quality and accuracy of the data stored in VIS, and, subsequently, the reporting as well. This may have adverse affects upon the final decision in relation to a visa application and to any subsequent applications lodged.

In addition to FTE concerns, the possibility of false matches, and their impact upon individuals, must be stressed. The EDPS has pointed out that an error rate of 0.5 - 1% is normal, which means that the checks system at external borders will have a False Rejection Rate (FRR) between 0.5 and 1%. Since the release of that opinion, technological developments have allowed for upgrades to the system; eu-LISA submits that the current FRR in verification processes is 0.2 - 0.3%, which, in an enormous database like the VIS, translates as more than 40,000 people whose identity may be wrongly verified. With regard to the identification process, there is no further information submitted, but false matches are directly related to the size of the system; the greater its capacity, the greater the danger of false matches. In the present case, the possibility of false matches is significantly heightened, since the VIS no longer contains a requirement for specific quality of data.

The possible consequences when fingerprints are matched erroneously during the fingerprinting process cannot be underestimated. On the one hand this may be done deliberately if an individual, whose digital fingerprints have been collected, does not otherwise disclose their real identity. In such cases of identity theft, the ‘hijacked’ identity will be permanently associated with the digital fingerprints in question. Furthermore, even in case of legitimate visitors, the impact of a false match may vary from a second line of checks comparable to the effect of non-verification of an EU passport, to ‘extremely grave, resulting in a rejection of a visa application or refusal of entry into the territory of Schengen States’.

The existence of rights to access and judicial remedies are certainly necessary in the long run, but may prove to be insufficient to mitigate these circumstances, as they may be time consuming. In the meantime, the individual affected may be obstructed in their free movement and in pursuing personal or professional activities, thus violating their private life.

940 VIS Regulation, art 8(5).
941 EDPS, ‘Opinion on the proposal for VIS Regulation’ (n352) 20.
944 EPEC, ‘Study for the Extended Impact Assessment’ (n773) 46.
945 Besides, national DPAS receive a rather modest amount of complaints. Council, Document 14365/15 (n866).
One could argue that the use of biometrics as a form of verification at the external borders may have the positive effect of shortening the timings of border crossings. However, this is not certain; border guards (as well as immigration authorities on national territory) may still consult a series of VIS data after the verification of the identity of a visa holder has been successful for the purpose of verifying the identity.946 Such consultation should have been reserved as a fallback procedure only in cases when the verification procedure has failed.947

The findings of the CJEU in Schwarz regarding the storage of fingerprints in a medium are important in the case of the VIS. Since 2007 the Regulation concerning the uniform format of visas requires Member States to include a photograph in order to increase document security and prepare for the introduction of the VIS.948 In 2003, the Commission proposed an amendment to that Regulation with a view to storing biometric data as well; in particular two fingerprints. Due to technical difficulties, the proposal was not formally adopted and the Commission withdrew it in 2006.949 Therefore, instead of storing biometric data on visa holders in a computer chip integrated into each visa sticker – in a process similar to the storage of fingerprints in a biometric passport – the technological limitations led to the centralised storage of biometrics. In light of Schwarz and the analysis in Chapter 2, storage of biometrics in a visa sticker on the one hand and in a centralised, multifunctional database on the other cannot be considered as interchangeable solutions. Furthermore, given that the preparations on the VIS had already commenced when this proposal was adopted and discussed, and the emphasis on the inclusion of biometrics as noted in the Thessaloniki European Council Conclusions, it is highly doubtful that even if a biometric visa sticker were possible, that centralised storage of fingerprints and photographs would have been avoided.

4.5.4 Retention period

The retention period is another key aspect for scrutiny, particularly as it attaches an element of continuity to the limitation to the right to privacy. In S and Marper, the Court called for defined retention periods, noting that the ‘perception that they are not being treated as innocent is heightened by the fact that their data are retained

947 EDPS, ‘Opinion on the proposal for VIS Regulation’ (n352) 22.
949 On the technical difficulties see Council, Document 6492/05 (17.02.2005).
indefinitely’.

As observed above, the duration of the storage period depends upon the type of the decision regarding the visa and its validity, if issued. Furthermore, although not explicitly mentioned, in cases of regular travellers to the Schengen area, a person’s file may be renewed on an indefinite basis. The VIS rules create the paradox that a SIS II alert on an irregular migrant may be reviewed and potentially erased after three years, whereas the personal information of legitimate travellers to the EU may be stored for much longer. However, the Regulation includes a catch-all approach without any selective criteria requiring differentiated retention periods. In fact, the more trusted a traveller is (since a visa has been issued), the lengthier the retention period is.

The ‘sweeping’ retention period is disproportionate, as it does not take into account the different situations that may occur in practice, nor the different types of visas under the scope of the VIS. In particular, cases where a visa applicant has been detected making duplicate or fraudulent visa applications may justify a longer retention period than in cases involving individuals whose visas have been issued and have travelled without any issues. This matter was actually proposed during the negotiations. However, Member States took the view that the five-year retention period was necessary, and even insufficient, particularly in view of the counter-terrorism function of the system. Furthermore, the retention period for applications that have been discontinued should also be re-evaluated. Differentiated treatment is also necessary in relation to refusal of visas. There are no compelling reasons why the data of a person whose visa has been refused due to administrative reasons should be stored for the same amount of time as those of a person whose application was refused for public security grounds. Another issue that must be considered is the alignment of the retention period of SIS II alerts with the VIS when the reason for a refusal is based on a SIS II alert.

Finally, advanced data removal could also have been extended to those third-country nationals who legally stay in Member States on the basis of long-stay visas and for persons that have obtained international protection.

### 4.5.5 Access and use of the VIS data

Further concerns are raised in relation to the use of VIS data. The risk of unauthorised access, fraud or falsification is considerable. In view of the wide range of

---

950 *S and Marper v UK* (n194) ¶122.
954 Ibid 18.
authorities granted access, which are not subject to further control at EU level, and the possibility of outsourcing in consulates, it becomes easier for officials who are neither equipped nor authorised to conduct searches. This increases the risks in maintaining control over how this information will be further used.

Moreover, the proportionality of use of the VIS to determine the merits of an asylum application is highly questionable. As Peers has eloquently observed, a record of refused visa applications, even if it involves a forged passport, could arguably indicate that the person concerned intends to enter and stay in the EU. However, it may equally show ‘the genuineness of that person’s desperation to flee persecution’. 955

Additionally, the possibility of transfers to third countries on an exceptional basis for the purposes of return raises proportionality concerns in three respects. Firstly, the fact that the existence of an adequacy decision constitutes one of the conditions for such transfer should be treated with caution, particularly in view of Schrems and the concerns regarding the privacy standards in the US. Secondly, one of the conditions involves the existence of general public interest grounds, 956 which is subject to national interpretation and may lead to divergent and potentially unlawful practices. 957 Finally, the safeguard on non-refoulement may be difficult to work in practice. 958

4.6 Proportionality of the VIS as a law enforcement tool

In order to comprehend the necessity of this ancillary objective of the VIS, the explanations provided in the preamble of the VIS Decision are central. There it is stated that:

‘[i]t is essential in the fight against terrorism and other serious crimes for the relevant services to have the fullest and most up-to-date information in their respective fields in order to perform their tasks. The Member States’ competent national services need information if they are to perform their tasks. The information contained in the VIS may be necessary for the purposes of preventing and combating terrorism and serious crimes and should therefore be available […] for consultation by the designated authorities.’ 959

955 Pees, EU Justice and Home Affairs Law (n475) 280.
957 Peers, EU Justice and Home Affairs Law (n475) 280.
958 ibid.
959 VIS Decision, recital 3.
As for access by Europol, it is pointed out that Europol ‘has a key role in the field of cross-border crime investigation and in supporting Union-wide crime prevention, analyses and investigation.’

This justification can be characterised, at best, as very weak. The fact that the information ‘may be necessary’ in the fight against terrorism and other serious crimes does not automatically mean that it must be available to law enforcement and Europol without further reasoning. The VIS was designed with a view to supporting the administration of visa policy and not as a police cooperation tool, which the judgment in UK v Council has made clear. In that sense, law enforcement access is not inherent in the system and constitutes a ‘significant change’, which should have been properly assessed in terms of its necessity and proportionality in the fight against terrorism and other serious crimes. The lack of an impact assessment study in this respect is an unfortunate choice that seems to suggest that such extension was almost taken for granted.

The consequences for visa applicants cannot be underestimated. Granting access to a former first pillar database to law enforcement agencies means that these third-country nationals are generally, and indiscriminately, suspected of being potential terrorists or criminal offenders, and are under a greater risk of being exposed to law enforcement measures or covert surveillance. Checks conducted within national territories and consultation of databases is generally based on risk assessments and profiling, which may enhance the risk of being further stigmatised and discriminated against. Visa applicants and holders are not treated on their own merit; irrespective of the legitimacy of their travel to the Schengen area and their personal profile, they are regarded as a potential threat.

Against this background, the VIS Decision allows consultation of the data solely for the purpose of the prevention, detection and investigation of terrorist offences and other serious crimes, as defined in other EU legal instruments. The definition of terrorist offences is currently under revision with a view to including a series of new criminal

---

960 ibid recital 4.
961 EDPS, ‘Opinion on the proposal for VIS Decision’ (n901) 2.
963 Evelien Brouwer, ‘Extraterritorial Migration Control and Human Rights: Preserving the Responsibility of the EU and its Member States’ in Ryan and Mitsilegas (eds), Extraterritorial Immigration Control (n2) 222.
acts as a response to the phenomenon of ‘foreign fighters’.\textsuperscript{964} The wide definition of terrorism has been kept, but the wording of terrorist acts is vague, thus raising legality concerns and leading to legal uncertainty.\textsuperscript{965} As for serious crimes, it could be argued that the barrier is rather low, since there is no further explanation regarding the specific penalty framework of the crimes encompassed.

Another point of concern relates to the authorities involved in the process of allowing access in criminal cases. By embracing a ‘broad and flexible wording’,\textsuperscript{966} Member States are left with wide discretion to determine which authorities are covered by the term ‘designated’ authorities\textsuperscript{967} subject to their organisational structure without further guidelines, requirements or limits other than that the functions of the authority must be related to the prevention, detection and investigation of terrorist or serious crimes, and the publication of an amendable list in the \textit{Official Journal of the EU}.\textsuperscript{968} No further review or control is foreseen at EU level. Access may therefore be potentially extended to a wide array of national authorities with diverse tasks.\textsuperscript{969} Furthermore, intelligence agencies whose mandate and functionalities are rather obscure are not explicitly excluded.\textsuperscript{970}

Admittedly, consultation of VIS data by law enforcement authorities cannot take place on a routine basis and is subject to clear-cut conditions on the basis of a pre-determined procedure. Therefore, at least \textit{in principle} there is no general power to search the entire system to produce ‘risk assessments’, or, in other words, to pursue fishing expeditions and profiling activities. Key in this respect is the intervention of a central access point as a verifying authority checking that the requirements for access are satisfied. Nevertheless, there is more to this than meets the eye. Firstly, the current wording on conditions leaves wide discretion for somewhat extensive access to police authorities. The threshold for allowing access could have been set higher by requiring

\begin{itemize}
\item \textsuperscript{964}See n883.
\item \textsuperscript{965}Some acts which have been criticised as broadly worded: inciting the distribution of a message to the public with the intent to incite the commission of a terrorist offence; inciting the financing of training for terrorism; aiding and abetting the soliciting of another person to participate in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way; travelling abroad for terrorism and organising or otherwise facilitating such travel. For comments see Standing Committee of Experts on International Immigration Refugee and Criminal Law (Meijers Committee), ‘Note on a proposal for a Directive on combating terrorism’ (CM1603, 2016).
\item \textsuperscript{966}Council Document 5456/1/07 (n893).
\item \textsuperscript{967}Brouwer, \textit{Digital Borders and Effective Rights} (n17) 132; Valsamis Mitsilegas, ‘The Border Paradox’ (n23) 58.
\item \textsuperscript{968}Notably, the list of ‘designated’ authorities is in most cases drafted in the official languages of the Member States only, thus making it difficult to draw conclusions.
\item \textsuperscript{969}Brouwer, \textit{Digital Borders and Real Rights} (n17) 132; Mitsilegas, ‘The Border Paradox’ (n23) 58.
\item \textsuperscript{970}ibid. Interestingly, the EDPS did not criticise this element, but he merely mentioned that it is welcomed that intelligence services are bound by the same rules as the rest of national authorities. EDPS, ‘Opinion on the proposal for VIS Decision’ (n901) 9.
\end{itemize}
the existence of factual indications as a basis for reasonable grounds. Despite it was then submitted that this condition could de facto make it impossible to access the VIS for the prevention of criminal offences, the substitution of ‘factual indications’ with ‘clear indications’ would have been a more balanced approach. Such an approach has been endorsed by the ECtHR in Zakharov v Russia. Furthermore, the specification of ‘danger’ associated with a crime would have limited the discretionary power of police agencies. Secondly, access to VIS data should have been made dependent upon the exhaustion of other sources, particularly information stored in other databases such as the national AFIS, and that of other Member States, pursuant to the Prüm Decision. This would have mitigated, at least to some extent, concerns that visa applicants are under suspicion of wrongdoing simply because their country of origin is listed among those subject to visa requirements. The third – particularly serious – concern relates to the functioning and independence of the central access point as a verifying authority. The VIS Decision does not provide much clarification as to the nature of such agencies and it is highly doubtful whether this procedure is fully independent or critical of police requests. Furthermore, the possibility of allowing more than one central access point is significant, as it leads to divergent understandings at the national level regarding the exceptional nature of access to VIS data. Indeed, the number of central access points designated at the national level considerably varies among Member States, spanning from 1 to 39. In Digital Rights Ireland, the Grand Chamber found that in order for competent national authorities to access telecommunications data, prior review must be carried out by a court or by an independent administrative body. However, such safeguards are nowhere to be found in the VIS Decision and thus compliance with privacy standards relies upon national interpretation and practice.

According to the latest report on the operation of the VIS, until late 2015 only 11 Member States reported that their designated authorities have consulted the VIS, having performed a total of 9,474 searches in accordance with the VIS Decision. 12 Member States did not report any criminal law activity, and Finland, the Netherlands and Slovenia have consulted the VIS for law enforcement purposes to a very limited extent, with less than 15 searches each. Over 38% of all searches were executed by Germany, followed by Hungary with almost 26%, Poland with almost 14%, and Spain with 11%

971 Mitsilegas, ‘The Border Paradox’ (n23) 58.
973 Council, Document 11062/06 (29.06.2006) 4.
974 Zakharov v Russia (n272) ¶255.
975 See Council, Document 11062/06 (n973) 8, which refers to ‘grave’ danger.
976 This is the case in Eurodac. See Chapter 4, Section 3.4.2.g.
977 Peers, EU Justice and Home Affairs Law (n475) 913.
978 eu-LISA, ‘VIS Report’ (n793) 34.
The aforementioned statistics could be read in multiple ways. On the one hand, the high discrepancies observed in national practice may mean that the concerns that the provisions leave room to a wide interpretation resulting in routine police access being allowed until now have not been substantiated. On the other hand, the low interest in the VIS could mean that there are not that many cases that require the assistance of the VIS, thus questioning law enforcement access altogether. Regrettably, the report does not provide further information as to the number of ‘hits’ on the basis of VIS searches, possible false matches, follow-up in cases of ‘hits’ and whether access by the central access points has been refused. Furthermore, there is no information as regards to the substantive grounds that rendered law enforcement access necessary. Some information in this respect is included in the Commission proposal for the establishment of the EES released in April 2016, where it is mentioned that:

‘[a]ccess to VIS data for law enforcement purpose has already proven its usefulness in identifying people who died violently or for helping investigators to make substantial progress in cases related to human being trafficking, terrorism or drug trafficking’. However, Member States have reported practical problems in the procedures to access the VIS by law enforcement authorities. Worryingly, the Commission has hinted at a revision of the conditions of access, with a view to lowering the already lax threshold enabling police authorities to consult VIS data on a more rigorous basis.

In relation to the conditions of access by Europol, the differentiated regime in comparison to national authorities is unjustified and, therefore, disproportionate. Access is broadly limited to its mandate and the performance of its tasks, and no search keys are foreseen. However, Europol’s objective is more general in nature and focuses on the improvement of the effectiveness and cooperation of competent authorities in Member States through information processing. The mere reference to Europol’s tasks means

\footnotesize

979 ibid 24.
980 Baldaccini (n23) 41.
981 The Commission was due to submit a report on the operation of the VIS, including its law enforcement aspects, by June 2016. In contact with the DG Home, the report will not be submitted until October 2016.
983 Commission, ‘Stronger and smarter information systems’ (n585) 9.
984 ibid.
985 See n908.
that consultation of VIS data is not restricted to specific cases \(^{986}\) and there is no need to substantially contribute to the purpose of the access. \(^{987}\) It could merely involve ‘enhancing the general information position of Europol or improving the quality of Europol data’. \(^{988}\) Furthermore, access is influenced by the Agency’s mandate, which is subject to modifications. \(^{989}\) This wide access by Europol defies the supposedly exceptional nature of law enforcement access, and may even lead to extensive risk assessments of visa applicants particularly in the context of analyses of a general or strategic nature. The lack of specific rules on supervision of Europol access to the VIS is regrettable in this respect. \(^{990}\)

The information that police authorities and Europol have access too, particularly in relation to people issuing an invitation and/or sponsoring a stay, also raises privacy concerns. Whereas such information may be relevant in certain cases for immigration control purposes, for law enforcement purposes it may result in extensive profiling by creating links between third-country nationals for the mere fact that they have established and developed personal relationships. The same applies to information on applications on a group of people applying together for a visa which, though excluded from the first set of data accessed, it will still be visible after a ‘hit’. Another important aspect in this respect that leads to the conclusion that police authorities may have rather extensive possibilities for profiling is the fact that the purpose of travel may be used a search key for conducting searches in the system. \(^{991}\)

Another central aspect involves the effectiveness of using biometric data in the fight against terrorist and other serious crimes through prevention. The extent to which the registration of such data in the VIS has a deterrent effect is doubtful. Terrorist organisations will always seek and develop methods to circumvent biometric border controls. \(^{992}\) Furthermore, in principle, terrorists do not use their own identity, or otherwise alter their personal details to make their identification difficult, and in many cases they have a substantial financial background allowing them to invest in skillful, unauthorised modifications to their travel documents, or otherwise allowing them to


\(^{987}\) Boehm (n32) 352.

\(^{988}\) Council, Document 5049/07 (04.01.2007) 4.

\(^{989}\) Boehm (n32) 351. Indeed, since the adoption of the VIS Decision, the legal framework of Europol has been twice revised. See n100.

\(^{990}\) Boehm (n32) 353.

\(^{991}\) EDPS, ‘Opinion on the proposal for VIS Decision’ (n901) 8.

\(^{992}\) Meijers Committee, ‘Consultation EU Visa Information System’ (n931) 3.
obtain high-quality fraudulent documents.\(^{993}\) With the collection and storage of biometric identifiers, perpetrators may be linked more easily to their true identity, unless they enter irregularly without obtaining a visa document, or provide a falsified travel document coming from a country where no visa is required. Therefore, the effectiveness of biometrics in the context of law enforcement is subject to two concurrent conditions: 1) that terrorists or organised criminals are nationals of a black-listed country, and 2) that they are known as such. Otherwise, the impact of police access is limited. Perhaps only in cases where fingerprints are found at a crime scene or after a terrorist attack would recourse to the VIS provide results in identifying individuals by their fingerprints, or provide further information about a suspect for the purpose of tracing them.\(^{994}\) In any case, the suspect must have made an application for a visa and their fingerprints must have been stored in the database. Furthermore, a possible false match by using fingerprints as search keys would have serious repercussions for a person wrongfully identified, possibly giving rise to their involvement in criminal investigations or even criminal proceedings. Given that the requirement of storing data that have passed a certain quality check has been dropped, the possibility of false matches becomes greater.

Finally, with regard to the transfer of data in urgent cases, it is regrettable that the Decision does not provide a definition or guidelines as to what constitutes an urgent case.\(^{995}\) In comparison to its \textit{lex generalis}, namely Framework Decision 2008/977/JHA that permits transfers without prior consent,\(^ {996}\) the VIS Decision requires consent of the Member State that entered the data. However, the lack of a rule according to which the level of data protection for the third party must be adequate for the intended data processing, as well as the expansion of access to a wide range of authorities globally, raises significant proportionality concerns.\(^ {997}\) The dangers are even greater in cases where poor quality data become at the disposal of agencies at a global level.

\(^{993}\) EPEC, ‘Study for the Extended Impact Assessment’ (n773) 20, 41-2, 59, 63.
\(^{994}\) Peers, ‘Legislative Update: Visa Information System’ (n853) 91.
\(^{995}\) Boehm (n32) 354.
\(^{996}\) Framework Decision 2008/977/JHA (n86) art 13(2), if such transfer is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and when prior consent cannot be obtained in good time.
\(^{997}\) Valsamis Mitsilegas, ‘Human Rights, Terrorism and the Quest for “Border Security”’ in Marco Pedrazzi and others (eds), \textit{Individual Guarantees in the European Judicial Area in Criminal Matters} (Bruylant 2011); Boehm (n32) 354.
5. Conclusion

The development of the VIS is a prime example of the trend towards preventive surveillance in EU immigration control, characterised by: increased targeting of migrants (and mobility in general); collection and storage of a wide range of personal information, including biometric data; and the blurring of boundaries between immigration and criminal law, by bypassing the specific purpose for which an instrument has been adopted. The VIS legitimised the tenuous link between extraterritorial immigration control and security prerogatives and introduced surveillance of movement of third-country nationals on an unprecedented scale. This shift in performing immigration control has considerably extended both the reach of the EU as a whole and of participating States raising significant privacy concerns. The VIS allows digital tracking of visa applicants through the mandatory collection of sensitive data, even if they never reach the Schengen territory, and the construction of profiles on the basis of everyday data, which reveal a wealth of information about their private life. This includes any personal relationships they may develop with EU nationals or other persons lawfully residing in the EU. In this context, all visa applicants are regarded as potential overstayers, or even criminals, on an indiscriminate basis, even if they have legitimate reasons for traveling, or have a perfect travel background. As such, the VIS maintains and accentuates the stigma placed on visa applicants by the imposition of a visa requirement to their country of origin, which seemingly is removed with the issuance of the visa sticker. However, as highlighted in Section 2, this stigma is somewhat ‘constructed’ based on various external relations issues, and not always related to risks of irregular migration or criminality.

This particularly serious interference with the right to private life is disproportionate to the overarching aim of implementing the EU common visa policy in multiple respects. To sum up the main points advanced in Section 4, it is submitted that the VIS Regulation requires the collection and storage of data on all visa applications in a generalised manner, without any exception, and irrespective of the personal circumstances of the individuals concerned. It must be recalled in this respect that the VIS is a largest catalogue of third-country nationals. In relation to each application file, a series of personal data are attached, even if these are not required for routine consultation. The inclusion of biometric data poses a series of proportionality concerns in light of their centralised storage, which leaves room for abuse and false matches in identification, with possibly significant repercussions to individuals. As such, and in

Mitsilegas, The Criminalisation of Migration in Europe (n8) 33.
view of the discriminatory effect it entails and their sensitive nature, it could be argued that their processing attacks the essence of privacy. The retention period does not make any differentiation between the different categories of visas or the different outcomes of the visa applications. Furthermore, the possible renewal of the application files may lead to *de facto* permanent cataloguing.

With regard to law enforcement access, it must be noted that the VIS legislative framework entails a complete disregard to the purpose limitation principle of data protection law, in that the mere possibility of police authorities having access to a system designed for visa policy purposes is not inherent to the nature of the system as visa policy tool. Admittedly, the rules on the law enforcement access to the VIS contain certain safeguards: there are certain limited conditions of access; a minimum of control by the central access point(s); and, as a general rule, transfers to third parties are prohibited. However, the provisions on law enforcement access allow for extensive interpretation. Furthermore, the independence of the central access point as a verifying authority is uncertain, particularly since in *Digital Rights Ireland*, the CJEU required a higher threshold for authorisation. In addition, the rules on access by Europol and on transfer of data to third parties are unclear. Besides, it must be observed that the possibility of false matches, which are enhanced in large-scale databases such as the VIS, entail serious repercussions for individuals who may be wrongfully implicated in criminal investigations.

In light of the above, the legislative framework of the VIS requires fundamental revision, whereby the massive collection of significant amounts of information from individuals who are, in principle, innocent must be re-evaluated as a policy choice, particularly since the gradual roll-out of the VIS is now complete and the database will steadily grow. Regrettably, as noted in Sections 3 and 4, the Commission contemplates revisions that will further deepen the feeling of surveillance to visa applicants. The registration of fingerprints of individuals above the age of 6 entails serious repercussions for minors and should not be seen as merely a technical matter. As for the relaxation of the conditions for law enforcement access in order to allow further ‘exploitation’ of the already stored data, it is noteworthy that already since 2012 concerns were expressed as to whether law enforcement authorities will demand access to the VIS data for purposes other than the ones of prevention, detection and investigation of terrorism and other serious crimes.999 Such revision will lead to further stigmatisation of visa applicants, as it will be easier for police agencies to solve more

---

easily cases related to individuals whose information is available rather than in cases related to persons whose data are not centrally stored.

The VIS has thus set a ‘bad’ precedent of identifying large groups of individuals whose movement is suspicious and must be tracked for a variety of divergent purposes, including criminal law related ones. The next Chapter, which is devoted to Eurodac, examines the monitoring of asylum seekers’ movements within the EU through fingerprinting, and discusses further the broad trend to grant law enforcement authorities access to immigration databases. The vulnerability of asylum seekers and the multiple reconfigurations of the database spanning three decades pose different privacy concerns, which merit further exploration.
CHAPTER 4. The Tale of Eurodac – An ‘Ugly Duckling’ Turning into a Swan?1000

‘In the EURODAC system the body of the asylum seekers becomes increasingly separated from an essential element of his or her legal personality, the right to be present. The body takes on an identity and is followed via its fingerprint data across borders while that part of the body’s legal personality which gives the right to be present remains trapped in one jurisdiction. The border of sovereignty in the end becomes the border of the essential human being. His or her data are captured in a database which establishes the border of movement for the purposes of the state.’1001

1. Introduction

Eurodac, which stands for European Dactyloscopy, is an pan-European database that processes the fingerprints of asylum seekers and certain categories of irregular migrants. Operational since 2003, this database constitutes the EU’s first experiment with biometric identifiers and was designed to assist in the implementation of the Dublin mechanism for the determination of the Member State responsible for examining an asylum claim. Under its current legal framework,1002 law enforcement authorities and Europol may access, under specific conditions, Eurodac fingerprints for the purpose of

1000 This Chapter is an extended and updated version of a book chapter entitled ‘The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?’ in Céline Bauloz and others (eds), Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System (Brill 2015).
1002 Regulation (EU) 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member States responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) [2013] OJ L180/1 (recast Eurodac Regulation).
preventing, detecting and investigating terrorist offences and other serious crimes, following the VIS model. The transformation of Eurodac is still ongoing; on 4 May 2016, the Commission adopted an amended proposal\(^\text{1003}\) essentially detaching Eurodac from its asylum framework and re-packaging it as a tool pursuing ‘wider immigration purposes’.\(^\text{1004}\)

Compared to other legal instruments of the so-called Common European Asylum System (CEAS),\(^\text{1005}\) Eurodac attracts rather modest interest, perhaps due to its inherently technical nature.\(^\text{1006}\) This Chapter focuses on the privacy concerns raised by the successive reconfigurations of Eurodac. Firstly, I map the historical overview of its legislative framework starting from its original conceptualisation in the 1990s to the 2016 recast proposal. Then, I examine the privacy challenges posed by the establishment and operation of Eurodac. Due to consecutive changes in the purpose of the database, I consider it appropriate to examine, in turn, the operation of the system as an asylum tool, as was originally envisaged, the comparison of Eurodac data for enforcement purposes, and its reinvigoration as an instrument broadly oriented towards immigration control.

2. **We need to talk about...Dublin**

As mentioned in Chapter 2,\(^\text{1007}\) among the ‘flanking’ measures for the dismantlement of internal border controls, the Schengen Convention stipulated rules on responsibility for asylum applications among the Schengen States. At EC level, Member

\(^{1003}\) Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless persons], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes (Recast version)’ COM(2016) 272 final (Eurodac proposal of 2016).

\(^{1004}\) ibid 6.


\(^{1007}\) See Chapter 2, Section 2.
States were confronted with similar challenges that the completion of the internal market would open up the possibility for asylum seekers to lodge their applications in two or more Member States, a phenomenon known as ‘asylum shopping’. The Dublin Convention of 1990 was signed in response of the abolition of intra-Member State border control and set out common rules on how to determine which Member State would be responsible for examining an asylum application. It superseded the refugee section of the CISA after its ratification in 1997, by which time all EU Member States had joined the Dublin system, alongside Norway and Iceland, which signed parallel agreements. The Dublin Convention was based on the ‘single application’ principle, according to which an application must be heard by a single Member State, and prescribed an allocation mechanism similar to the Schengen rules comprising of a hierarchy of criteria. Such criteria included the existence of a family member of the applicant who was a recognised refugee in another Member State, the issuance of a residence permit or a visa by a certain Member, and the rule that responsibility would go to the Member State from where the asylum seeker first entered the EU. As Guild has observed, responsibility for examining an asylum claim has thus been treated ‘as a burden and a punishment for the Member State which permitted the individual to arrive in the Union’. The basic principles underpinning the Dublin system remain to date, albeit twice amended. The Convention was substituted by the Dublin II Regulation in 2003, which included certain additions and amendments to the responsibility rules. In 2013, the Dublin III Regulation was adopted as part of the second

1009 Convention determining the state responsible for examining applications for asylum lodged in one of the Member States of the European Communities [1997] OJ C254/1 (Dublin Convention).
1011 Dublin Convention, art 3(2).
1012 ibid arts 4-8.
1013 ibid art 4.
1014 ibid arts 5(1) and 5(2).
1015 ibid art 6.
1017 Regulation 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national [2003] OJ L50/1 (Dublin II Regulation).
1018 Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) [2013] OJ L180/31 (Dublin III Regulation).
generation of the CEAS. On 4 May 2016, the Commission tabled a recast proposal on the Dublin mechanism, which is currently under discussion.1019

From its early days the Dublin mechanism attracted heavy criticism, not least because it separated family members and forced asylum seekers to destroy their travel documents with a view to avoiding the application of the conflict rules, as there would be no proof about which countries they had previously entered.1020 This latter issue has been consistently raised by Member States, which claim that asylum seekers lie about how they arrived in the country or their nationality, pretending to be nationals of ‘refugee-producing’ countries.1021 From the State perspective, a key practical question has been how to establish that someone is really who he claims to be, and, in lack of travel documents, how to assign a person a certain identity.1022 Furthermore, the lack of documentation prevented Member States from establishing the route travelled and determining whether they had applied for asylum in another country. The possibility offered by biometrics to use a person’s body and store the data in a large computerised database became appealing, as it could at least ascertain ‘the identity of the person in front of them and his or her movement within the EU from the time first “tagged”’.1023 As van der Ploeg has pointed out, fingerprinting must be understood as a practice of establishing identity rather than examining the preexisting one, ‘in the sense that “identity” becomes that which results from these efforts’.1024 This process could settle whether asylum seekers belonged territorially and jurisdictionally to the place they physically were, by framing them as risks that justify further control.1025 Thus came the first pan-European fingerprint database, Eurodac.

1019 Commission, ‘Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)’ COM(2016) 270 final (Eurodac proposal of 2016).
1021 Guild, ‘Unreadable papers?’ (n1001) 32.
1022 ibid.
1023 ibid.
1024 van der Ploeg (n1006) 300.
1025 Gammeltoft-Hansen (n4).
3. Eurodac: The ‘truth serum’ of the EU asylum policy

3.1 The early days

The need to establish a centralised system containing the fingerprints of asylum seekers was on the agenda since the early stages of the Dublin cooperation. In December 1991, Immigration Ministers first expressed their interest in setting up a European system to compare dactyloscopic data of asylum seekers, which led to the release of a feasibility study in 1992. In November 1992, the Ministers decided to look into the necessity and requirements of Eurodac and asked the Council Legal Service whether Article 15 of the Dublin Convention could be used as the legal basis for establishing the system. The Council Legal Service confirmed so, but marked that the data could not be used for other purposes, such as ‘the functioning of other international instruments or for starting criminal investigations against asylum seekers’.

In November 1995 the die had been cast: Eurodac was technically feasible and so legislative preparations could proceed. At that time, ten of the then 15 EU Member States were already fingerprinting asylum seekers and storing their fingerprints in national registers. With the establishment of Eurodac, such practices became institutionalised and formalised. As Aus has observed, Member States therefore uploaded domestic standards to the supranational level in a ‘bottom up’ process. During the second half of 1997, the draft Eurodac Convention was forwarded for consultation to the Parliament. By that point, the basic rules on the functioning of the system had been agreed upon and the system would be confined to comparing asylum

---

1026 For a detailed overview of the story behind Eurodac see Aus, ‘Eurodac’ (n1006); Steve Peers and Nicole Rogers (eds), EU Immigration and Asylum Law (Martinus Nijhoff 2006) 263-8.
1028 Council, Documents 1284/92 REV 2 (01.12.1992); 1419/93 WGI 1365 (02.1993). Article 15 of the Dublin Convention prescribed the exchange, upon request, of individual data necessary for the examination of an asylum application, for the establishment of the Member State responsible for such an application and for other obligations stemming from the Convention.
1030 Council, Document 11476/95 ASIM 308 (23.11.1995). As noted by Aus, ‘the technical feasibility of Eurodac preceded a political assessment of the project’s desirability and appropriateness.’ Aus, ‘Eurodac’ (n1006) 7 (emphasis original).
1032 Brouwer, ‘Eurodac’ (n1006)
1033 Aus, ‘Eurodac’ (n1006) 14.
seekers’ fingerprints only. In its resolution, the Parliament stressed, among other aspects, that the use of the database must under no circumstances be expanded to cover wider areas or purposes than those falling within very strict limits.

Negotiations progressed and in March 1999 the Council agreed to expand the material scope of Eurodac through a special Protocol, extending the fingerprinting obligations to ‘illegal immigrants’. This addition, which was prompted by the migratory and refugee wave of mid-1997, particularly from Iraq and other States, received mixed reactions from Member States. Central in the discussion was whether both irregular entrants and irregular residents would be included within the scope ratione personae. On the one hand, Germany, Austria, the Netherlands and the UK favoured the extension to irregular residents, but on the other hand, France, Belgium and Luxembourg found this systematic recording equated asylum seekers with irregular migrants and preferred to avoid an ‘uncomfortable amalgam’ of asylum and migration issues. To solve these discrepancies it was decided that whereas the Protocol would mandate the registration of fingerprints for those irregularly entering the EU, with regard to irregular residents Member States would enjoy discretion.

In view of the Amsterdam Treaty shortly coming into force, the negotiations froze in wait of a new EC instrument based on Article 63(1)(a) TEC that the Commission would present. The proposal was released in May 1999 and, after a year of discussions, Regulation 2725/2000 was adopted, complemented by Regulation 407/2002.

---

1035 Peers and Rogers (n1026) 263.
1037 ibid. Notably these amendments involved increased parliamentary control over the system and ensuring the rights of asylum applicants.
1038 ibid 132.
1039 Council, Documents 5945/98 (13.02.1998); 6191/98 (20.02.1998); 6191/1/98 (27.02.1998).
1040 The choice of a Protocol was preferred in order not to delay the signing of the Convention. Peers and Rogers (n1026) 264.
1041 ibid.
1042 Aus, ‘Eurodac’ (n1006) 7-8.
1043 van der Ploeg (n1006) 299.
1044 For the negotiations see Council, Documents 10221/98 (19.07.1998); 11646/98 (01.10.1998); 4595/98 (07.10.1998).
1046 For an analysis see Aus, ‘Eurodac’ (n1006) 10. The negotiations proved harsh resulting in an amended proposal which required re-consultation of the EP. The latter suggested raising the age limit from 14 years to 18, but this amendment was disregarded by the Council.
3.2 The Eurodac Regulation

Eurodac has been intrinsically linked to the operation of the Dublin mechanism. According to Article 1 of the Regulation, the purpose of the database was:

‘to assist in determining which Member State is to be responsible pursuant to the Dublin Convention for examining an application for asylum lodged in a Member State, and otherwise to facilitate the application of the Dublin Convention under the conditions set out in this Regulation’.

In order to track secondary movements in the EU, the Regulation obliged Member States to promptly collect the fingerprints of every asylum seeker over the age of 14 when they applied for international protection. The collected fingerprints would be stored in the Central Unit – a central database established within the Commission – where they would be compared with fingerprints that had already been transmitted and stored by other participating countries. Eurodac would be equipped with an AFIS and would function on a hit/no hit basis, meaning that the transmitted data would be automatically checked against other stored fingerprints and in case of a match, a notification would be given. If a Eurodac check revealed that the fingerprints had already been recorded in another Member State, the latter could be requested to take back the asylum applicant on the basis of the Dublin rules.

Furthermore, Member States were under the obligation to collect the fingerprints of all third-country nationals apprehended ‘in connection with the irregular crossing by land, sea or air of the Member State’ and transmit them to the Central Unit for comparison against fingerprints subsequently collected from asylum seekers. Therefore, the fingerprints of persons apprehended irregularly crossing the external border would neither be compared against the fingerprint data previously taken by other irregular border-crossers and asylum applicants, nor with that of irregular border-

1049 This age was the lowest common denominator, but the Netherlands wished to lower it to the age of 12. Council, Document 10191/3/97 (27.11.1997).
1050 Eurodac Regulation, arts 4-7.
1051 ibid art 4(5).
1052 According to the Council, this concept is controversially extended to cases involving third-country nationals ‘apprehended beyond the external border’ where they are still en route and there is no doubt that they crossed the external border irregularly. Council, Document 12314/00 ADD 1 (15.11.2000). Therefore, as Busch has observed, ‘the obligation to take fingerprints […] is not limited to the external border itself’. Nicholas Busch, ‘EU Law-making after Amsterdam: The Example of Eurodac’ (Fortress Europe Circular Letter, 1999) http://www.fecl.org/circular/5901.htm accessed 15 August 2016.
1053 Eurodac Regulation, arts 8-10.
crossers that were subsequently collected and transmitted. According to Council statements, the obligation would be confined to cases ‘where there is no doubt that the crossing was made irregularly’, meaning that the irregular crossing had to be ‘recent and proven’. As for ‘aliens found illegally present’ on national territory, their fingerprints could be collected and checked against the system to determine whether they had previously applied for asylum in another Member State. However, neither Member States were obliged to undertake the procedure, nor would the data be centrally stored.

Apart from a full set of fingerprints, Eurodac would store limited information on the sex of asylum seekers and irregular border crossers, the date of registration and transmission of fingerprints to the Central Unit, and the Member State of origin. The person’s name, nationality or date of birth would not be included and, thus, the individual would be defined by no more than their fingerprints. Each set of data would be stored for a period of ten years from the date on which the fingerprints were collected. If, in the meantime, an asylum seeker would be recognised as a refugee, the data would be ‘blocked’ – but not deleted – meaning that a ‘hit’ would not be transmitted. Otherwise, data would be erased upon expiry of the retention period or in the event that an asylum seeker acquired citizenship of any Member State. As for the data on irregular border-crossers, the retention period was two years, but could be erased early if the person was issued a residence permit, left the EU or acquired EU citizenship.

With regard to individual rights, the person concerned would have to be informed by the Member State of origin of the identity of the controller, the purpose for which the data would be processed, the recipients of such data, the obligation to provide their fingerprints, and the existence of rights to access and rectification of their data. Furthermore, rights of correction and erasure were foreseen, for which responsibility

---

1054 House of Lords – European Communities Committee, ‘Fingerprinting Illegal Immigrants: Extending the Eurodac Convention – 10th Report of Session 1998-1999’ (1999) ¶54. 1055 ibid. 1056 Eurodac Regulation, art 11. 1057 ibid art 11(3). 1058 ibid arts 5(1), 8(2). 1059 Guild, ‘Unreadable Papers? (n1001) 32. 1060 Eurodac Regulation, art 6. 1061 ibid art 12. This rule was transitional. According to Article 12(2), five years after Eurodac would become operational, the EU institutions would decide the fate of those data on the basis of statistics. 1062 ibid art 7. 1063 ibid art 10. 1064 ibid art 10(2). 1065 ibid art 18. It is explicitly noted that such an obligation shall not apply if proven impossible or would involve a disproportionate burden.
would go to the Member State that transmitted the data.\textsuperscript{1066} According to Articles 18(11) and 18(12) of the Eurodac Regulation, third-country nationals were entitled to bring an action or complaint before the competent authorities or national courts if their rights were refused. Finally, supervision over the lawfulness of the processing was entrusted to national DPA’s and the Joint Supervisory Authority, which was substituted by the EDPS.\textsuperscript{1067}

As the Eurodac Regulation was the first instrument adopted under the Amsterdam rules, it was a test case regarding the application of special rules on the territorial scope of measures falling within the then Title IV TEC. When the database became operational on 15 January 2003, with the exception of Denmark (which was automatically excluded pursuant to Articles 1 and 2 of the Protocol on the position of Denmark annexed to the EU Treaties),\textsuperscript{1068} all EU Member States were connected to the system. This included the UK and Ireland, which decided to opt in; Norway, Iceland, Switzerland and Liechtenstein also participate as Dublin Associate States.\textsuperscript{1069}

3.3 Law enforcement access to Eurodac data: A record-breaking issue

The idea of allowing law enforcement authorities to consult asylum seekers’ fingerprints is attributed to the German Government in the aftermath of 9/11.\textsuperscript{1070} In 2004, just one year after Eurodac had begun functioning, the Hague Programme called for the maximisation of effectiveness of EU information systems, and ‘an innovative approach to the cross-border exchange of law enforcement information’.\textsuperscript{1071} In November 2005, the Commission published a Communication on improved effectiveness, enhanced interoperability and synergies among databases stating that ‘authorities responsible for internal security could […] have access to Eurodac in well-defined cases, when there is a substantiated suspicion that the perpetrator of a serious
crime had applied for asylum’. A few months later, the political will to grant police access to Eurodac was expressed at the G-6 meeting of March 2006 in Heiligendamm. The German Presidency of the first half of 2007 reasoned this approach in its programme on police and judicial cooperation as follows:

‘Frequently, asylum-seekers and foreigners who are staying in the EU unlawfully are involved in the preparation of terrorist crimes, as was shown not least in the investigations of suspects in the Madrid bombings and those of terrorist organizations in Germany and other Member States […] The police and law enforcement authorities therefore need greater access to EUROPADAC, because in many cases this is the only way of identifying suspected offenders or of detecting aliases of suspects. Access to EUROPADAC can help provide […] with new investigative leads making an essential contribution to preventing or clearing up crimes’.

After pushing for the drafting of a proposal amending the Regulation of 2000, the Commission was invited to table a proposal in June 2007. The Commission drafted no less than four proposals (in 2008, 2009, 2010 and 2012), which makes Eurodac the record-holder of being the first, and only,
legislative instrument that was recast that many times before its adoption. However, only the proposals of 2009 and 2012 contained rules on access by law enforcement authorities to Eurodac data. The proposal of 2009 introduced the possibility of law enforcement authorities having access to Eurodac in relation to ‘the prevention, detection, and investigation of terrorist offences and other serious criminal offences’.\footnote{Commission, ‘Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of “EURODAC” for the comparison of fingerprints for the effective application of Regulation (EU) No […] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)” COM(2012) 254 final (Proposal of 2012).}

Due to the then pillar structure of the EU, a proposal for a third-pillar decision concerning law enforcement access accompanied a proposal for a first-pillar Regulation. However, the proposals were severely criticised, especially by the EDPS,\footnote{EDPS, ‘Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of “EURODAC” for the comparison of fingerprints for the effective application of Regulation (EC) No […] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law Enforcement authorities and Europol for law enforcement purposes’ [2010] OJ C92/1.} and were eventually blocked by the Parliament.

With the entry into force of the Lisbon Treaty, and the abolition of the pillar structure of the EU, the proposal for a Decision lapsed. With a view to speeding up the negotiations on the completion of the CEAS, the proposal of 2010 did not refer to law enforcement access to Eurodac data. However, no political agreement was reached. Therefore, Austria, backed by nine other Member States, insisted on re-introducing the provisions on law enforcement access, since Eurodac was perceived as an important tool in combating crime.\footnote{Council, Document 16006/10, (09.11.2010) 2.} In May 2012, the Commission released a fourth proposal in an attempt to put an end to the Eurodac saga. After a limited period of negotiations, the Parliament – in a profound shift – backed the Council and the recast Regulation was adopted in June 2013. The 180° turn of the Parliament must be seen in light of the pressure to conclude the negotiations for the CEAS. As MEP Ska Keller has noted, the recast Regulation is:

‘the result of a cheap horse trade with the Council: The police of the Member States are granted access to Eurodac so that they can in turn agree
to at least a few improvements of the mutual EU standards for asylum procedures and the accommodation of asylum seekers’

3.4 The recast Eurodac Regulation

3.4.1 Operation of Eurodac as an asylum tool

In view of the dual purpose of the database as an asylum management and a law enforcement instrument, the recast Regulation is legally based on Articles 78(2)(e), 87(2)(a) and 88(2)(a) TFEU concerning asylum and police cooperation policies. The basic rules on the function of Eurodac have remained relatively unchanged. The scheme currently comprises: a) a Central System, now managed by eu-LISA, which is a central database in which data are processed for the purpose of comparing the fingerprints taken by participating States, and b) a communication infrastructure between the Central System and Member States. Each Member State has a single National Access Point through which communication between the central and the national part is established. In addition to certain terminological changes, the recast Regulation introduces a specific time frame of 72 hours within which Member States must transmit the fingerprint data to the Central System and extends the scope to cover all applicants for international protection by including those seeking subsidiary protection. In case a ‘hit’ leads to the transfer of an applicant to another Member State pursuant to Dublin rules, the receiving State must insert a new dataset into the

---


1085 Recast Eurodac Regulation, art 4.

1086 ibid art 3(1).

1087 ibid art 3(2). For the latest list of competent authorities see, eu-LISA, ‘List of designated authorities which have access to data recorded in the Central System of Eurodac pursuant to Article 27(2) of the Regulation (EU) No 603/2013, for the purpose laid down in Article 1(1) of the same Regulation’ (2016).

1088 ibid arts 8 and 11. The term ‘aliens’ has been replaced by the term ‘third-country nationals’.

1089 Ibid arts 9(1), 14(2). This was added in order to address the issue whereby Member States delayed the transmission of fingerprints and in the meantime, asylum seekers had already lodged their application in another Member States, resulting in ‘hits’ in wrong sense. For an overview see Brigitte Kuster and Vassilis Tsianos, ‘How to Liquefy a Body on the Move: Eurodac and the Making of the European Digital Border’ in Raphael Bossong and Helena Carrapico (eds), Shifting Borders of European Union Internal Security: Technology, Externalisation and Accountability (Springer 2016).

1090 Recast Eurodac Regulation, art 2(1)(a).
The retention period for storing the data of irregular border-crossers is reduced to 18 months, given that the Dublin II Regulation reduced the time period for which a Member State is responsible for dealing with an asylum application to one year. As for the fate of fingerprints collected from beneficiaries of international protection – an issue that the original Regulation left for future determination – these are neither automatically blocked nor deleted, but ‘marked’ for a period of three years. This means that these data remain at the disposal of national authorities and upon the expiry of the three-year period they are blocked until their deletion. Finally, in relation to individuals’ rights, the recast Regulation provides for certain additions to the right of information; the obligation to inform applicants about the secondary use of the data in the law enforcement context and the duty to supply them with a leaflet setting out information on their rights.

On 20 July 2015, the recast Regulation came into force. Compared to the rest of the large-scale information systems, Eurodac is the most widely operational database, functioning in 32 European countries. According to the latest statistics of 2015, Eurodac has processed 789,872 fingerprints of applicants for international protection, and 274,936 fingerprints of migrants apprehended irregularly crossing borders. Furthermore, 187,478 fingerprints of irregular residents have been transmitted for comparison, primarily from Germany. 202,552 ‘hits’ have been reported in relation to asylum seekers’ data, and 248,806 ‘hits’ in relation to irregular border-crossers.

### 3.4.2 Consultation by law enforcement authorities and Europol

The key change brought about by the recast Regulation is that national police bodies and Europol are permitted to consult Eurodac data for the purposes of preventing, detecting or investigating terrorist offences and other serious crimes. As in the case of the VIS, terrorist crimes correspond, or are equivalent, to those referred to in

---

1091 ibid arts 10(a), (b).
1092 Dublin II Regulation, art 12. This rule is maintained under Dublin III Regulation, art 13(1). The Commission proposal foresaw full alignment in this respect. Commission, ‘Proposal of 2012’ (n1080) art 16. Member States wished to maintain the two-year retention period for law enforcement purposes. Council, Document 11861/12 (06.06.2012) 55.
1093 Recast Eurodac Regulation, art 18. See n1061.
1094 ibid art 29(1)(b).
1095 ibid art 29(3).
1097 ibid.
1098 ibid 6.
1099 ibid 7.
Articles 1 to 4 of Framework Decision 2002/475/JHA on combating terrorism. Serious crimes are specified in Article 2(2) of Framework Decision 2002/584/JHA on the EAW if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years. Due to the duality of the Eurodac functions, the data protection rules applicable in this context are those of Framework Decision 2008/977/JHA which is the lex generalis, but where the Regulation itself provides for data protection safeguards, it prevails as lex specialis.

The latest available statistics from eu-LISA on law enforcement access to Eurodac data reveal that between 20 July 2015 and 31 December 2015 only five Member States (Austria, Germany, the Netherlands, France and Finland) requested consultation of the system in 95 cases. No information has been released as to whether these consultations have resulted in a ‘hit’, the circumstances of the cases or whether these matches have been followed up at the national level. Until the end of 2015, Europol had not yet been connected to the system, and, to the best of my knowledge, such connection has still not yet taken place. As for the modalities of access, these are outlined below.

a) Authorities involved

According to Article 5 of the recast Regulation, Member States shall designate the authorities to be granted access to Eurodac for criminal law purposes. In a definition matching the one used in the Decision granting access to law enforcement bodies to the data stored in the VIS, designated authorities are those ‘responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences’. Agencies or units exclusively responsible for intelligence relating to national security are verbatim excluded. Furthermore, lists of the designated authorities, and the operating units within the designated authorities, are kept by each Member State.

The recast Regulation stipulates that a verifying authority is entrusted with the role of checking that the conditions of access are fulfilled. This body is a single authority, or a unit of such an authority, among those responsible for the prevention, detection or

---

1100 See n882-883.
1101 See n596.
1102 Recast Eurodac Regulation, art 2(1)(k).
1103 See n86.
1104 Recast Eurodac Regulation, recital 39, art 33.
1107 Recast Eurodac Regulation, art 5(1).
1108 ibid art 5(2) and (3).
1109 ibid art 6.
investigation of terrorist offences and other serious crimes. Furthermore, in accordance with Recital 30 of the Regulation, the designated and verifying authority can be within the same organisation. Originally, there were no clarifications regarding the nature and structure of this body. However, the Parliament expressed concerns about the autonomy of such a body in performing its tasks. It thus proposed an explicit reference to the need for independence of the authority, which should not receive instructions from the designated authorities regarding the outcome of the verification process.\textsuperscript{1110} In recognition of the danger, this suggestion was incorporated into the final wording of Article 6. However, there seems to have been a particularly strong concern about this threat, as the reference to the independence of the verifying authority is emphasised by its replication three times in the Preamble\textsuperscript{1111} and a fourth time in Article 6. As for Europol access, a specialised unit within the organisation, but acting independently, will take the role of the verifying authority.\textsuperscript{1112}

b) Procedure

If a designated authority (or Europol) wish to request comparison of fingerprint data with those already stored in Eurodac, they must follow a specific procedure. In particular, according to Article 19(1), they must submit a reasoned electronic request to the verifying authority via the National Access Point. After verification that the conditions for the request are met, the National Access Point will process the request transmitted by the verifying authority to the Eurodac Central System.\textsuperscript{1113} It is noteworthy that once the verifying authority has determined that the conditions are fulfilled there is no other mechanism to ensure compliance with EU standards apart from the periodical monitoring by the national DPA,\textsuperscript{1114} because the verifying authority does not transmit the reasons provided by the designated authorities to the National Access Point.\textsuperscript{1115} Furthermore, in exceptional urgent cases, in order to prevent an imminent danger relating to a terrorist offence or other serious crime, a request can be transmitted to the National Access Point and verification that conditions have been met will be provided ex-post and ‘without undue delay’.\textsuperscript{1116} The wording of this provision was adopted at the behest of the Parliament,\textsuperscript{1117} since the proposal did not include any

\begin{itemize}
\item \textsuperscript{1110} Council, Document 7476/13 (15.03.2013) 90-2.
\item \textsuperscript{1111} Recast Eurodac Regulation, recital 29 (twice) and recital 30.
\item \textsuperscript{1112} ibid art 7(1).
\item \textsuperscript{1113} ibid art 19(2).
\item \textsuperscript{1114} Information discussion with Commission Officer (Brussels, November 2014).
\item \textsuperscript{1115} ibid recital 29.
\item \textsuperscript{1116} Commission, ‘Proposal of 2012’ (n1080) art 19(3).
\item \textsuperscript{1117} Council, Document 5155/13 (11.01.2013) 131.
\end{itemize}
remark as to what qualifies as an exceptional case of urgency, a point that could potentially lead to diverging interpretations and uncertainty.\textsuperscript{1118}

c) Conditions of access

With regard to the conditions of access, national authorities are not given a \textit{carte blanche}. Requests for consulting Eurodac data are permitted ‘in specific cases and when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences’.\textsuperscript{1119} The specificity of a case arises in particular when the request for comparison is connected to a specific and concrete situation or danger associated with a terrorist offence or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that they will commit or have committed any such offence. In addition, a specific case exists when the request for comparison is connected to a person who is the victim of a terrorist offence or other serious criminal offence.\textsuperscript{1120} The latter reference marks a significant difference between Eurodac and VIS rules in that the former may be also be used in cases where asylum seekers are not suspected of being the perpetrators of offences.

According to Article 20(1) of the recast Regulation, three conditions must be fulfilled in order for the designated authorities to have recourse to Eurodac data. Firstly, they must have consulted national fingerprint databases, as well as the AFIS of other Member States pursuant to Decision 2008/615/JHA (Prüm Decision)\textsuperscript{1121} and the VIS, and such consultation must have been futile. In the case of AFIS, such comparisons must have taken place where technically available, unless there are reasonable grounds to believe that a comparison with such systems will not lead to the establishment of the identity of the data subject.\textsuperscript{1122} Recital 32 explains that this situation may arise when ‘a case does not present any operational or investigative link to a given Member State’.


\textsuperscript{1119} Recast Eurodac Regulation, recital 31.

\textsuperscript{1120} ibid; compare with Document 16982/06 (n1076) according to which law enforcement access was to be ‘based on factual indications for believing that the data subject has committed or will commit a [serious] criminal offence’.


\textsuperscript{1122} This provision partly reflects the opinion of certain Member States which suggested that instead of a comprehensive procedure including a comparison with all Member States’ national databases, targeted Prüm queries should suffice according to the specifics of each case. Council, Document 14559/12 (04.10.2012).
Besides, the need to implement the Prüm Decision is a prerequisite for granting access to Eurodac data. Furthermore, the Regulation requires that the comparison must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, which means that there must be an overriding public security concern which makes the searching of the database proportionate. The comparison must be necessary in a specific case and there must be reasonable grounds to consider that the comparison will *substantially* contribute to the prevention, detection or investigation of any of the criminal offences in question. Such reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence is an asylum seeker whose data is recorded in the database. As in the case of the VIS, no routine access to the database is allowed, which means that unless these conditions are fulfilled, law enforcement authorities cannot have access to Eurodac data as part of their investigative powers.

As for the conditions of access by Europol, Article 21(1) of the recast Regulation prescribes that comparison of fingerprint data is allowed within the limits of Europol's mandate and when it is necessary for the performance of the Agency's tasks. In addition, comparisons with fingerprint data stored in any information processing systems that are technically and legally accessible by Europol must not have led to the establishment of the identity of the data subject. Furthermore, the comparison must be necessary in order to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate. This means that there must be an overriding public security concern, which makes the searching of the database proportionate. The remaining conditions are the same as for Member States. Besides, the Member State that recorded the data must authorise the processing of data by Europol. In comparison with the proposal of 2012, which followed the VIS model, the conditions for access have been largely improved and elaborated in order to match the respective conditions for Member States' authorities and address the criticisms that were raised in relation to the proposal.

---

1123 The addition of the word ‘substantially’ was the subject of debate. In the proposal of 2009 this reference is included, yet in the proposal of 2012 was omitted. For criticism see EDPS, ‘Opinion on the Eurodac proposal of 2012’ (n1118) ¶57; Meijers Committee, ‘Note on the Eurodac proposal of 2012’ (n1118) 6; Council, Document 5155/13 (n1117) 134. Emphasis added.

1124 Eurodac Regulation (n 3) Article 21(3).

d) Transfer of data

Transfers of data to third countries, international organisations or private entities established in or outside the EU are forbidden.\(^{1126}\) This prohibition also applies if the data is processed further at the national level or between Member States pursuant to Framework Decision 2008/977/JHA.\(^{1127}\) Furthermore, personal data that originated in a Member State and is exchanged between Member States following a ‘hit’ should not be transferred to third countries if there is a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment, or any other violation of their fundamental rights.\(^{1128}\) Nevertheless, these provisions do not apply to third States to which the Dublin III Regulation applies.\(^{1129}\) As explained in Recital 41, the prohibitions serve to ensure the right to asylum and to protect asylum seekers from having their personal data processed by a third country. This is why the same Recital clarifies that apart from fingerprint data, other data stored in the database must not be transferred. The rules on transfers of data to third parties were adopted under pressure from the Parliament,\(^{1130}\) which sought to address concerns regarding the ambiguity of the previous wording of the Regulation that appeared to allow for loopholes which could potentially result in asylum seekers’ data ending up in third countries.\(^{1131}\)

e) Latent fingerprints

Finally, an important addition to the Eurodac rules is the possibility for law enforcement authorities to conduct searches of Eurodac based on latent fingerprints. These are fingerprints left on a surface which was touched by an individual and may be found at a crime scene.\(^{1132}\) This is the first time in which latent fingerprints can be used for search purposes; the legislative framework of the VIS does not provide for such possibility.

\(^{1126}\) Recast Eurodac Regulation, art 35(1).
\(^{1127}\) See n86.
\(^{1128}\) ibid art 35(2).
\(^{1129}\) ibid art 35(3).
\(^{1130}\) Council, Document 5155/13 (n1117) 197.
\(^{1132}\) As mentioned in Recital 14 of the recast Regulation, the use of latent fingerprints is a ‘fundamental facility for police cooperation’.
3.5 Eurodac under pressure – The massive influx of refugees and migrants

At the time when the recast Eurodac Regulation became effective, the massive influx of refugees and migrants escalated and certain Member States, particularly Greece, became overwhelmed with fingerprinting those arriving at the external borders.\footnote{1133} Failure to comply with their obligations under the Eurodac Regulation, particularly in relation to the obligation to transmit the relevant data to the Central System within 72 hours, became a frequent phenomenon attributed to infrastructure deficiencies or unwillingness of State authorities to take responsibility.\footnote{1134} Exemplary of the deficiencies experienced is the fact that the Commission has initiated infringement proceedings against Greece, Croatia and Italy for incorrect implementation of the Regulation.\footnote{1135} Furthermore, another source of ‘gaps’ in registration related to the lack of cooperation particularly on behalf of Eritreans and Syrians that have refused to have their fingerprints collected and stored. This issue, which must be seen as a collateral effect of Dublin coercion, resulted in diverging practices at the national level, spanning from coercion to detention. In order to address these challenges, in its European Agenda on Migration the Commission highlighted that ‘Member States must […] implement fully the rules on taking migrants’ fingerprints at the borders’.\footnote{1136} In this respect, it provided guidelines to facilitate systematic fingerprinting\footnote{1137} and contemplated the collection of other biometric identifiers, particularly digital photos.

Whilst certain Member States have been under pressure, in those Member States that are not situated at the external borders increasingly came the desire to be able to store and compare information on irregular migrants that were found irregularly staying on their territory, particularly when they did not seek asylum. In other words, they

\footnote{1133} For an overview see Parliament, ‘Fingerprinting migrants: Eurodac Regulation’ (PE571.346, 2015).
sought to extend the reach of Eurodac so that the information on irregular migrants would not be used solely for asylum-related purposes.

3.6 The 2016 Commission proposal

On 4 May 2016, the Commission tabled an amended proposal on Eurodac, as part of a first package of a broad reform of the CEAS. The proposal signals a landmark change in Eurodac’s purpose from being a system ensuring the effective implementation of the Dublin mechanism into an instrument serving wider immigration purposes, including the return of irregular migrants. This idea dates as far back as 2004, when the Council considered the use of biometrics for return-related purposes as a best practice to clarify the identities of persons being returned. According to the proposal, in addition to the existing objectives, Eurodac will:

‘assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation’.

The re-package of Eurodac as a multi-purpose tool derives from the need to strengthen the EU’s return policy with regard to irregular migrants and to keep track of them if they make movements across the EU. This change affects a series of provisions. In particular, on top of a full set of fingerprints, Member States shall be obliged to take and transmit a facial image in relation to all three categories falling within the personal scope of Eurodac. Therefore, for the first time since the establishment of the database, information on persons who were found irregularly present will be centrally stored. The age threshold for children is significantly reduced to the age of six, an issue which, as mentioned earlier, is contemplated also in relation to the VIS. In the case of Eurodac, this change is meant to assist in the identification of minors in cases

---

1138 See n1003.
1141 ibid art 2(1) 2016. These fingerprints may be collected and transmitted at the discretion of Member States by members of the European Border Guard Teams or EASO experts. This article further permits Member States to introduce sanctions for those individuals who refuse to comply with the registration procedure.
1142 ibid art 2(2). Rules have been added to ensure that the collection of fingerprints from minors is carried out in a child-sensitive and child-friendly manner.
1143 See Chapter 3, Section 3.2.2.
where they are separated from their families or abscond from care institutions or child social services.\textsuperscript{1144}

The categories of data held in the database are also considerably expanded, in order to ‘allow immigration and asylum authorities to easily identify an individual, without the need to request this information directly from another Member State’.\textsuperscript{1145} Thus, from a biometric system, Eurodac will essentially get closer to the VIS paradigm by storing the following additional information: In relation to asylum seekers, the data set recorded shall include: a) facial image; b) name (or known alias); c) nationality; d) place and date of birth; e) information on travel or identity document; f) asylum application number; g) allocated Member State; and h) where applicable, the date of transfer to the allocated Member State.\textsuperscript{1146} In relation to irregular border crossers and irregular residents, the system will store the elements under (a) – (d) as described above, as well as the date when the person concerned left or was removed from EU territory.\textsuperscript{1147} The inclusion of facial images in Eurodac is intended to mitigate the risk that fingertips are damaged, even deliberately, to prevent a ‘hit’, and to address the inadequacies in technical infrastructure at the national level on the one hand, and resistance on the part of some asylum seekers or irregular migrants to comply with the fingerprinting procedure on the other.\textsuperscript{1148} To ensure the accuracy of a ‘hit’, both sets of biometric data – fingerprints and facial images – would have to be compared. The proposed Regulation would, however, allow comparisons to be based solely on facial images as a last resort in circumstances where an individual’s fingertips are too damaged to ensure a high level of accuracy, or the individual concerned refuses to provide fingerprints.\textsuperscript{1149}

In view of the expanded aims of Eurodac, the rules on procedure are streamlined; once fingerprints and photos of asylum seekers and irregular migrants are taken and transmitted to the system, they will be automatically compared to the ones already transmitted and stored.\textsuperscript{1150} This will enable national authorities to check whether a person apprehended crossing the external border irregularly was ever present in a Member State, whether an irregular migrant has claimed asylum elsewhere or has entered another Member State irregularly. As such, Eurodac will enable the construction of patterns of irregular or secondary movements throughout the EU\textsuperscript{1151} by following the

\textsuperscript{1144} Commission, ‘Eurodac proposal of 2016’ (n1003) explanatory memorandum, 10.
\textsuperscript{1145} ibid 13.
\textsuperscript{1146} ibid art 3.
\textsuperscript{1147} ibid arts 13-4.
\textsuperscript{1148} ibid explanatory memorandum, 13.
\textsuperscript{1149} ibid arts 15-6.
\textsuperscript{1150} ibid art 15(1).
\textsuperscript{1151} ibid explanatory memorandum, 13.
chronology of an immigration narrative from the EU periphery to the core. In any case, a Dublin ‘hit’ will be prioritised.1152

The retention period for the fingerprints and facial images of asylum seekers remains unchanged,1153 to ensure that Member States can track secondary movements within the EU following a grant of international protection status where the individual concerned is not authorised to reside in another Member State’.1154 As for the retention period of irregular migrants’ data, it is set at five years, aligned to that prescribed in other databases and to the length of an entry ban under the Return Directive.1155 Deletion of data before the expiration of the retention period is foreseen solely when the person acquires the citizenship of an EU Member State.1156 Irregular migrants’ data will not be deleted, but will be marked when obtaining a residence permit.1157

Additionally, the draft Regulation foresees the transfer of data solely for the purpose of identifying and re-documenting in the process of return and readmission.1158 Such transfer is based on two cumulative conditions: a) the third-country national explicitly agrees to do so, and b) the Member State of origin gives its consent. No information on the fact that an asylum application has been lodged shall be disclosed. The data could be used to track unauthorised secondary movements of refugees or other beneficiaries of international protection, as well as asylum seekers and irregular migrants, making it possible to transfer an individual back to the Member State that originally granted protection.

Finally, streamlining the rules on the different categories of persons falling within the remits of the database also signifies that law enforcement authorities and Europol will get their hands on the much larger Eurodac jar. However, no further amendments to the conditions of access have been proposed. Of course, this does not eliminate the possibility that such amendments will not be discussed during the negotiating phase, particularly after the evaluation of the VIS shall be released in autumn 2016. Quite the contrary, the Commission has already announced that the modalities of access to Eurodac will be reconsidered with a view to providing for simplified procedures so that law enforcement access can take place more rigorously.1159

1152 ibid art 15(4).
1153 ibid art 17(1).
1154 ibid explanatory memorandum, 14.
1155 ibid arts 17(2) and (3).
1156 ibid art 18.
1157 ibid art 19.
1158 ibid art 38.
1159 Commission, ‘Stronger and smarter information systems’ (n585) 9.
4. Evaluation of Eurodac in light of Article 7 EUCFR

4.1 Assessing the establishment of Eurodac as a tool to facilitate the Dublin mechanism

4.1.1 Application of Article 7 EUCFR

The operation of Eurodac is currently based on the recording and further processing mainly of fingerprints, and no other personal data such as the name, address or nationality are registered in the system. Taking into account S and Marper and Schwarz, it is clear that the collection and storage of asylum seekers’ and irregular border crossers’ fingerprints constitutes a limitation to their right to private life. The case of Eurodac paved the way for fingerprinting to acquire a routine character, even though at that time it was deployed at national level only. Third-country nationals within the scope of the Regulation cannot be considered as having consented to the registration of their fingerprints. Pursuant to Article 9 of the recast Regulation, in order for an asylum seeker to lodge an application for international protection, it is compulsory to register their fingerprints to Eurodac. Furthermore, pursuant to Article 14 of the recast Regulation, Member States are obliged to fingerprint third-country nationals apprehended crossing the external border irregularly, and to transmit the collected data for comparison. This obligatory character is further exemplified by the Guidelines provided by the Commission, whereby if the person concerned has applied for asylum, but refuses to cooperate in being fingerprinted, Member States may consider their detention to determine or verify their identity or nationality on the basis of the Directive 2013/33/EU on reception conditions of asylum seekers. Coercion is also foreseen as a measure of last resort if all other practicable alternative measures have been exhausted. The delimiting character of mandatory registration of fingerprints is further enhanced due to their storage in a centralised EU-wide database. However, this does not mean, in the case of third-country nationals found irregularly staying on national territory, that the mere collection of fingerprints does not amount to a limitation of privacy. Since the taking of fingerprints is combined with a comparison to those already registered in the system and may result in similar effects as storage

---

1160 Commission, “Implementation of the Eurodac Regulation as regards the obligation to take fingerprints” (n1137) 3-4.
1162 Commission, “Implementation of the Eurodac Regulation as regards the obligation to take fingerprints” (n1137) 4.
(Dublin transfer), I consider that also in their case, their fingerprinting is sufficient to consider that the right of private life is limited.

4.1.2 Essence of privacy

In Chapter 3,\textsuperscript{1163} it was submitted that the mass collection and further processing of biometric data of unsuspected persons for a multiplicity of purposes could be considered as going to the core of privacy, particularly when it involves a huge pool of individuals. Whereas with regard to the initial use of Eurodac as an asylum tool this proposition does not seem to be applicable, the current reconfigurations of Eurodac, and particularly the recent proposal, seem to fall within the definition since the system follows closely the example of the VIS.

4.1.3 Objective of general interest

The next criterion to be scrutinised is whether Eurodac genuinely meets an objective of general interest recognised by the EU. As observed in Chapter 1, this criterion is understood more broadly in the EU context than in the ECHR, which provides an exhaustive list of legitimate aims. In \textit{Schwarz}, the Court contended that the prevention of illegal entry into the EU is such an objective without the need to assign it to one of the aims included in Article 8(2) ECHR.\textsuperscript{1164} By analogy, the facilitation of implementing the Dublin provisions and the development of a common asylum policy in the EU with a view to prevent ‘forum shopping’ or asylum seekers in orbit must also be considered as an EU objective of general interest.

However, before the EUCFR acquired binding effect, and even before its proclamation, the existence of a legitimate aim on the basis of Article 8(2) ECHR was a confusing matter, leading academics to note that ‘there is no ground which clearly applies’.\textsuperscript{1165} The underlying rationale of Eurodac seems to be based on a rather disturbing intertwining of asylum seeking with criminality, also exemplified by the fingerprinting process which carries connotations of wrongdoing. The UK Government asserted that the primary justification of Eurodac is the prevention of crime, noting that

\textsuperscript{1163} See Chapter 3, Section 4.2.
\textsuperscript{1164} \textit{Schwarz} (n320) ¶37-8.
\textsuperscript{1165} Brouwer, ‘Eurodac’ (n1006) 243-4; Peers and Rogers (n1026) 268.
crossing a border irregularly is not only a crime in itself, but ‘it would often also involve the commission of other offences of forgery and deception and "generate serious criminal behaviour on the part of others"’.\textsuperscript{1166} Furthermore, the fingerprinting process could be justified by reference to the prevention of disorder criterion; if the Dublin system broke down, asylum seekers could cross the weakest border irregularly and then travel to the Member State where it would be easiest to acquire refugee status, thus resulting in disorder and possibly impinging upon the rights of asylum seekers who had genuine reasons for applying for asylum.\textsuperscript{1167}

### 4.1.4 Is the limitation ‘provided for by law’?

Since the fingerprinting rules are prescribed in the Eurodac Regulation, in principle, the processing of fingerprints is provided for by law. As explained in Chapter 1, this criterion entails that the legislation in question is of sufficient precision to allow individuals to sufficiently foresee its effects. Whereas in relation to asylum seekers the precision of rules appears sufficient, as regards irregular migrants this criterion has not been fully respected. The main point of concern is the definition of persons to be fingerprinted when apprehended ‘in connection with the irregular crossing of the external border’ which is broadly worded. The precision of the term is called all the more in question given that during the negotiating phase, the Council seemed to foster a wide meaning of this definition, which includes persons apprehended even beyond the external border.\textsuperscript{1168}

### 4.1.5 Proportionality test

In \textit{Schwarz}, the Court found that the collection and storage of fingerprints is an appropriate means to prevent, \textit{inter alia}, illegal entry into the EU, taking the view that the possibility of false matches will merely draw the competent authorities’ attention to the person concerned and will result in a detailed check of that person with a view to definitely establishing their identity.\textsuperscript{1169} The case of Eurodac is fundamentally different, not only because the centralised storage in a large-scale system increases the risk of

\textsuperscript{1166} House of Lords, ‘Fingerprinting Illegal Immigrants’ (n1054) ¶43.
\textsuperscript{1167} ibid ¶45.
\textsuperscript{1168} Peers and Rogers, \textit{EU Immigration and Asylum Law} (n1026) 269. See n1052.
\textsuperscript{1169} \textit{Schwarz} (n320) ¶44.
false matches, but also because the impacts of a false match to an asylum seeker is far more serious, thus raising concerns regarding the appropriateness of fingerprinting. A Eurodac ‘hit’ presumes that the person in question has arrived through the territory of another Member State and thus in principle may be sent back to that country. Indeed, according to Article 22 of the Dublin III Regulation, in order for Member States to determine the responsibility for an asylum claim, a Eurodac ‘hit’ serves as probative evidence and, unsurprisingly, most of the Member States rely heavily on such evidence to base their Dublin requests. In fact, some Member States only accept Eurodac hits as evidence of their responsibility. Furthermore, it has been reported that national authorities may not sufficiently examine family ties if a Eurodac hit is obtained, as this seems to take precedence despite the hierarchical order of the Dublin criteria. This blind trust on biometric identification disregards not only its limitations, but also entails that a wrongfully – or even a correctly – transferred person may be subjected to national asylum systems in which their treatment would be substantially different both in terms of reception conditions and in terms of asylum claim determination. Besides, the impact on the individual who has been wrongly transferred, the delays in hearing their case, and the overall uncertainty on their status also cannot be underestimated.

Furthermore, the inextricable link created between the Dublin mechanism and Eurodac signifies that the latter derives its necessity from the proper implementation of the former; if the Dublin system is not functioning properly, the fingerprinting process must be called into question. By now, the failure of Dublin is well known and broadly accepted. The system is not ‘working’ either for asylum seekers or for Member States in at least three respects. Firstly, asylum seekers who enter the EU through its periphery (i.e. Italy, Greece) defy the Dublin rules and move on to the EU core to lodge their asylum application elsewhere. This secondary movement should not be seen as ‘asylum shopping’, but rather as a means of seeking humane reception conditions and

---

1170 Brouwer, Digital Borders and Real Rights (n17) 141.
1172 ibid.
1173 ibid 31, 42, 47.
1174 For a narrative of a case concerning the wrongful transfer of a Sudanese from the UK to Italy on the basis of wrong identification see Guild, ‘Unreadable Papers?’(n1001) 42-3. Clayton reports two cases before the UK Tribunal, in YI [2007] UKAIT 00054 and RZ [2008] UKAIT 00007 concerning the reliability of biometrics, where the Courts held that the accuracy and evidential weight of fingerprint evidence is susceptible to challenge. Gina Clayton, ‘The UK and Extraterritorial Immigration Control’ in Ryan and Mitsilegas (eds), Extraterritorial Immigration Control (n2) 405-6.
procedures that do not fall short of international and EU standards.\textsuperscript{1177} Therefore, the deterrent effect of fingerprinting, as highlighted above, has not worked as a decisive factor. Secondly, Dublin is mistakenly premised on the existence of asylum standards across the EU Member States that are equivalent, or at least comparable. Quite the contrary, both recognition rates\textsuperscript{1178} and reception conditions\textsuperscript{1179} differ to the extent that both the CJEU\textsuperscript{1180} and the ECtHR\textsuperscript{1181} have released landmark rulings condemning appalling reception conditions. The systemic deficiencies in Greece have even led to the suspension of Dublin transfers since 2011, thus further questioning why there is a need to store asylum seekers’ or irregular border crossers’ fingerprints in an EU-wide database, since Dublin transfers will never (or rarely) take place. The case of Greece is not the sole example. Available statistics demonstrate that during the period 2008-2012, only around 25\% of outgoing requests resulted in transfers, meaning that Dublin transfers take place in only around 3\% of asylum cases in the EU.\textsuperscript{1182} The most recent Commission evaluation of the Dublin III Regulation confirms the very low number of transfers in comparison to the number of Dublin requests.\textsuperscript{1183} In light of the above, I consider that the failings of Dublin have a domino effect to the operation of Eurodac, stripping away its necessity. Since the allocation mechanism is problematic and, therefore, must be fundamentally reformed, the need for maintaining the instrument assisting in this allocation, namely Eurodac, must also be seriously reconsidered.

Another point of concern involves the impact of the fingerprinting process on asylum seekers and irregular migrants. In Schwarz the CJEU found that the collection of two fingerprints for the purposes of issuing an EU passport is proportionate taking into account that it does not ‘cause any particular physical or mental discomfort to the person affected any more than when the person’s facial image is taken’.\textsuperscript{1184} This is not arguable in the case of Eurodac. As highlighted in MSS v Belgium and Greece,\textsuperscript{1185}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{1177} Elspeth Guild and others, ‘Enhancing the Common European Asylum System and Alternatives to Dublin’ (PE519.234, Parliament 2015) 55.
\item \textsuperscript{1180} Joined Cases C-411/10 and C-493/10 NS v Secretary of State for the Home Department and ME and Others v Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform [2011] ECR I-13905.
\item \textsuperscript{1181} MSS v Belgium and Greece (2011) 53 EHRR 2; Tarakhel v Switzerland (2015) 60 EHRR 28.
\item \textsuperscript{1182} Guild and others, ‘New Approaches’ (n1175) 9.
\item \textsuperscript{1183} Commission, ‘Evaluation of the implementation of Dublin III Regulation’ (n1171) 56-7.
\item \textsuperscript{1184} Schwarz (n320) ¶48.
\item \textsuperscript{1185} MSS v Belgium and Greece (n1181) ¶233.
\end{itemize}
\end{footnotesize}
asylum seekers constitute an inherently vulnerable group of individuals who have often fled their country of origin to escape war or persecution, and may have experienced significant hardships crossing the sea in overcrowded and unsafe boats in fear for their lives. It indicates an approach whereby police logic is creeping, and applicants for international protection and irregular migrants carry the mark of illegality. In this context, they may not feel comfortable in registering their fingerprints for various reasons; it may be partly attributed to an avoidance attitude induced by Dublin coercion, but it may well be that asylum seekers have had bad experiences with providing their fingerprints to the police in their countries of origin, or that they fear the fingerprints may be shared with their country of origin which could endanger family members. In turn, lack of cooperation may lead to their deprivation of liberty through detention, and even physical or psychological coercion, to overcome resistance as a means to force people to register their fingerprints, which could lead to a risk of re-establishing feelings of trauma and victimisation. Such practices implicate other fundamental rights alongside privacy, such as the risk of inhuman or degrading treatment or punishment and the right to liberty. In other words, in an attempt to protect one’s privacy, limitations to other rights may occur.

Be it as it may, the fingerprinting process of asylum seekers has always been a tenuous issue, not least because the need to record of a full set has never been explained. Additionally, it is hard to justify why migrants apprehended irregularly staying on national territory should be covered by the scope ratione personae of the Regulation. Already at the negotiating stage, the Council Legal Service opined that ‘the inclusion in Eurodac of data relating to persons who legitimately crossed the external frontiers of a Member State, but had later been found residing unlawfully in a Member State cannot be justified’. The Council explained in this respect that data on irregular residents may be communicated to Eurodac if:

‘- the alien declares that he (she) has lodged an application for asylum in a Member State;
- the alien does not request asylum but objects to being returned to his (her) country of origin by claiming that he (she) would be in danger, or otherwise seeks to prevent his/her return by showing no identity papers’.

From this latter reference, it is evident that even at that time Eurodac went beyond its

---

1186 Guild and others, ‘New Approaches’ (n1175) 57.
1188 ibid 7.
1189 Council, Document 8441/98 (18.05.1998).
1190 House of Lords, ‘Fingerprinting Illegal Immigrants’ (n1054) ¶57.
mission to serve as a tool for Dublin purposes. JUSTICE noted in this respect:

‘[I]f Member States consider it necessary to take and exchange fingerprints of individuals who object to being returned to their country of origin on grounds of fear this should be included on the face of a separate Council act (or new Title IV instrument), subject to the requirements of Article 8(2) of the European Convention on Human Rights’.

In any case, it has been rightly pointed out that there is an ‘insufficient link’ between the comparison of fingerprints and the application of the Dublin Convention unless there is substantial evidence of a prior claim to asylum in another Member State. If no such indication exists, there is no need to take or compare fingerprints.1191

The retention period of fingerprints must also be examined in light of the Courts’ pronouncements in *S and Marper* and *Digital Rights Ireland*. From its inception, the retention period of datasets in Eurodac fluctuates depending on the category of third-country nationals whose fingerprints are stored. The rules in relation to both asylum seekers and irregular migrants apprehended crossing the external border raise proportionality concerns. On the one hand, the storage of asylum seekers’ fingerprints for ten years has never been properly justified even though the Parliament suggested reducing it to five years, an amendment that was ignored by the Council.1192 The lack of justification is further exemplified from the fact that in the 2016 proposal for amending Eurodac the Commission kept this rule without any re-evaluation, claiming that ‘Member States can track secondary movements within the European Union following a grant of international protection status where the individual concerned is not authorised to reside in another Member State.’1193 On the other hand, the retention period of irregular border crossers’ data is dependent upon the Dublin rules regarding the period for which a Member State remains responsible for an asylum applicant. Article 6 of the Dublin Convention stipulated that the responsibility of the Member State the borders of which were crossed irregularly ended when a person had resided in another Member State for six months before lodging an asylum application. Therefore, the two-year retention period was clearly disproportionate and data should not have been kept for more than 18 months, because it would not be legally possible for that data to facilitate the application of the Dublin rules. The Dublin II Regulation replaced this rule and, according to its Article 12(1), responsibility for an asylum claim ceases 12 months after the date on which the irregular border crossing took place. Although the Commission suggested a decrease in the retention period, Member States initially insisted on

---

1191 Peers and Rogers (n1026) 270.
1192 See n1046.
maintaining the existing timeframe but settled for the 18-months, although this is also disproportionate, as it does not correspond to the Dublin rules.

4.2 Assessing the comparison of Eurodac data for law enforcement purposes

4.2.1 Law enforcement access: A separate limitation to privacy with far reaching consequences

Since the beginning of discussions on law enforcement access to Eurodac data, numerous academics, Tzanou (n31) 194-9; Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), ‘Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac’ (CM0712-IV, 2007); ‘Note on the Eurodac proposal of 2012’ (n1118). 1194 the UNHCR,1195 and the EDPS1196 have condemned deviation from the original purpose of the database and the significant implications of this deviation for the fundamental rights of asylum seekers. Much of this criticism has centred on the possibility of function creep or through the erosion of the purpose limitation principle. In the ECHR context, this issue was highlighted in Weber and Saravia v Germany,1197 where the Strasbourg Court stressed that the transmission of data to, and their use by, other authorities, which enlarges the group of persons with knowledge of the personal data, constitutes a further separate interference with the fundamental right of private life. In the present case, it is particularly worrisome that thousands of applicants for international protection, who underwent fingerprinting for asylum purposes only, have their fingerprints used for an additional purpose which was unknown to them at the time of registration, with possible significant repercussions for them.1198

1194 Tzanou (n31) 194-9; Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), ‘Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac’ (CM0712-IV, 2007); ‘Note on the Eurodac proposal of 2012’ (n1118).
1195 UNHCR, ‘An Effective and Protective Eurodac’ (n1131).
1196 EDPS, ‘Opinion on the Eurodac proposal of 2009’ (n1082); ‘Opinion on the Eurodac proposal of 2012’ (n1118).
1197 Weber and Saravia v Germany (n260) ¶79.
1198 As noted by the Meijers Committee, apart from a separate limitation to privacy, opening up Eurodac may even affect asylum seekers’ right to request international protection enshrined in Article 18 EUCFR. Access by Europol is key in this respect; the Agency may use information from third countries, received on the basis of operational agreements as an indication of ‘proving reasonable grounds to consider a comparison with Eurodac data will lead to the identification of a victim or suspect of serious crime in a specific case’. Therefore, asylum seekers run thus the risk of being labelled as terrorists or suspected criminals by their countries of origin, thus preventing them from securing international protection in the EU. Meijers Committee, ‘Note on the Eurodac proposal of 2012’ (n1118) 3.
Undoubtedly, the use of asylum seekers’ fingerprints for law enforcement purposes signifies a radical transformation of the database from a merely administrative tool into an instrument of criminal intelligence gathering.\(^{1199}\) By default, it disregards the fact that asylum seekers constitute a particularly vulnerable group of people who require a high level of protection,\(^{1200}\) and deepens the already disturbed relationship of distrust between states and asylum seekers. Furthermore, it should be seen as symptomatic of a wider trend to allow law enforcement authorities access to EU databases that were not originally designed for that purpose, as analysed in the case of the VIS. Importantly, it is another prime example of preventive justice through risk, whereby emphasis is placed on identifying unknown threats by assigning risk to different suspect populations.\(^{1201}\) Eurodac, as a risk technology, could thus be redeployed from the asylum domain to the domain of the fight against terror in an attempt ‘to feign control over the uncontrollable’.\(^{1202}\) This focus on prevention is more than rhetoric; as the Belgian delegation noted, the preventive use of the Eurodac system ‘might lead to abuses’.\(^{1203}\)

Given the profound deviation from the original purpose of data collection that these measures relating to access for law enforcement agencies represent, and the vulnerability of asylum seekers being singled out as a group of particular interest for criminal enforcement, the interference with privacy must be considered as particularly serious. This means that when the Regulation stipulates the proportionality and necessity of law enforcement access, it must be kept in mind that the threshold to be invoked is particularly high.

4.2.2 Necessity of law enforcement access - flawed design of national databases or a flawed perception of asylum seekers?

Strikingly the references to the necessity of granting access to law enforcement agencies are minimal. Recital 8 of the recast Regulation merely states that:

‘[i]t is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and


\(^{1201}\) Louise Amoore and Marieke de Goede (eds), Risk and the War on Terror (Routledge 2008).


\(^{1203}\) Council, Document 11861/12 (n1092) 1. Also see Council, Document 14847/12 (18.10.2012).
most up-to-date information if they are to perform their tasks. The information contained in Eurodac is necessary for the purposes of the prevention, detection or investigation of terrorist offences [...] or other serious criminal offences.’

In comparison to VIS, the EU legislature is more assertive, but a connection between asylum seekers and criminality, such as that inevitably made by the Regulation, implies that asylum seekers as a group of people are targeted for compelling reasons, and that such reasons ought to be adequately explained. Law enforcement access is not merely ‘a technical exercise,’ As the EDPS has eloquently noted:

‘Just because the data has already been collected, it should not be used for another purpose which may have far-reaching negative impact on the lives of individuals. To intrude upon the privacy of individuals and risk stigmatising them requires strong justification and the Commission has simply not provided sufficient reason why asylum seekers should be singled out for such treatment.’

This is true; the Impact Assessment accompanying the 2009 proposal did not provide for specific examples where access to Eurodac by law enforcement authorities and Europol would be beneficial. The Impact Assessment merely explained that searching fingerprints through the national AFIS of other Member States using the Prüm Decision was not fully reliable, because some Member States may not store the fingerprints of asylum seekers in their national AFIS unless they were related to crime. Furthermore, Framework Decision 2006/960/JHA could only be used to collect data on asylum seekers if there were factual reasons to believe that the information was actually available in a specific Member State, and mutual legal assistance could be time consuming. However, the prioritisation of the implementation of already existing opportunities for information exchange should have taken place before creating new channels for exchanging information. Given the significant implications in terms of

---

1204 Compare with Chapter 3, Section 4.6.
1206 ibid.
1207 Commission, ‘Staff Working Document – Impact Assessment accompanying Document to the amended proposal for a Regulation of the European Parliament and the Council concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation No […]/[…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version) and to the Proposal of a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes’ SEC(2009) 936 final (Impact Assessment of 2009) 8.
1208 See n802..
fundamental rights, a thorough evaluation of existing instruments should have been carried out so as to ensure they were indeed insufficient. This would have also been in line with the Stockholm Programme, which highlighted that ‘increased attention needs to be paid in the coming years to the full and effective implementation, enforcement and evaluation of existing instruments’. 1211

The proposal of 2012 was not accompanied by a fresh Impact Assessment, even though the first attempt to allow law enforcement access to the database was blocked by the Parliament. Besides, the initial Impact Assessment was already out of date, as it did not take into consideration any developments regarding the implementation of existing information exchange mechanisms. The only information thus available regarding the necessity of law enforcement access is the submissions of three Member States, namely Austria, the Netherlands and Germany, which were the principal proponents of law enforcement access to Eurodac data. 1212 In particular, the Dutch pointed out that between 2007 and 2011 access to the national asylum seekers’ fingerprints database was permitted in 356 cases, and in 134 cases (38%) such comparison led to one or more criminal identifications. 1213 Furthermore, in Germany, where the national AFIS includes the fingerprints of both asylum seekers cases and criminal cases, around 40% of criminal identifications resulted from a comparison with the fingerprints data of asylum seekers. 1214 No further details on the number of these cases are available. Moreover, in Austria, which applies the same system as Germany, between 2007-2011 criminal identifications were possible in 310 cases. These submissions do not include any information on the criminal proceedings themselves nor final convictions. Furthermore, the feedback from Germany and Austria does not concern terrorism and serious crime only, but all types of offences. 1215 As for access by Europol, there was no reference to existing cases in which there were reasonable grounds to assume that access to Eurodac would aid in the prevention, detection or investigation of terrorist attacks. 1216 As the JSB of Europol has noted, it did not see any evidence from the Commission to prove such access was necessary. 1217

Given this fragmentary information, no definite conclusions can be drawn as to whether or not access to Eurodac is necessary for fighting terrorism and serious crime. However, the submissions from Member States, coupled with the reasons provided by the Commission when explaining the necessity for law enforcement access, raise

1211 Stockholm Programme (n606) ¶1.2.2.
1213 ibid 3.
1214 ibid 4.
1215 Eechaudt (n1076) 8.
1217 JSB of Europol (n1125) 2.
significant concerns regarding the perception of asylum seekers at national level. It appears that at least six Member States and two other States that implement the Dublin acquis keep asylum seekers’ fingerprints in their AFIS.\textsuperscript{1218} This ‘merging’ design of national databases in certain Member States seems to have acted as a ‘stumbling block’ in certain respects. In particular, when a Member State wishes to consult information available in other Member States under Prüm, if the latter State has opted for a unified database, which contains information on both criminals and asylum seekers, then the requesting state automatically has access to data on asylum seekers. However, the requested Member State does not have that option. It comes as no surprise that the Member States which were pushing for the use of asylum seekers’ fingerprints in criminal cases were those whose national AFIS contained both asylum seekers’ and criminals’ data.\textsuperscript{1219} It thus appears that the way domestic AFIS are constructed in some Member States, and the consequent lack of reciprocity in what is available in all Member States, had a significant impact in the adoption of the measure. As mentioned above, the EU legislator considers that the Prüm system is insufficient because some Member States do not store asylum seekers’ data with those of criminals. The mere fact that in certain Member States asylum seekers’ data is stored within a unified database along with data on criminals is particularly worrying. This approach indicates that asylum seekers form a suspect population whose data should be available for processing in the context of law enforcement, and this view is institutionalised and supported at EU level. In this context, the example of the recast Eurodac Regulation demonstrates how certain Member States have used EU policies to make their own internal problem of how their national AFIS were designed into an EU problem. It also echoes and extends to asylum policy the argument of Geddes that ‘European cooperation and integration have helped EU member states consolidate and reassert their ability to regulate international migration through the use of new EU-level institutional venues’.\textsuperscript{1220} By allowing the police to have access to Eurodac data, the recast Regulation essentially remedies any inequalities in information exchange among Member States caused by the aforementioned ‘merging’ design of specific national AFIS.

\textsuperscript{1218} Commission, ‘Impact Assessment of 2009 (n1207).
\textsuperscript{1219} In relation to the Dutch example see Brouwer, ‘Eurodac’ (n1006) 243.
4.2.3 Proportionality of law enforcement access

Be it as it may, it must be stressed that law enforcement access may lead to increased stigmatisation of asylum seekers. The mere existence of the possibility of law enforcement authorities and Europol having access to Eurodac data indicates that applicants for international protection are considered as de facto persons suspected of criminality. This perception is enhanced by the fact that their fingerprints are kept for a significant period of time, even after their recognition as beneficiaries of international protection, and may influence the way society treats such individuals. Asylum seekers who have committed no crime could face a greater likelihood of being involved in criminal investigations than other individuals whose biometric data are not collected, stored and processed on a systematic basis for the sole reason of having applied for asylum, a right to which they are entitled to. Due to this possibility, asylum seekers who committed crimes could be discovered more easily, leading to an apparent increase in the rates of offences committed by asylum seekers, and thus indicating a high level of criminality among them. However, such possibility does not exist for other categories of individuals, since no such databases for other groups of people exist, at least for the time being. In this respect, Eurodac differs from VIS in that it targets individuals who are in principle situated within the EU territory, whereas VIS targets tourists who, in the majority of cases, have crossed the EU external border at some point. In any case, the impression would be faulty, as the statistics would be based on the access to fingerprint data on all asylum seekers and only the sporadic fingerprint data available on other groups of the population. This increased exposure of asylum seekers to criminal investigation disregards the principle of the presumption of innocence and could potentially fuel acts of xenophobia and racism on the basis of false notions that asylum seekers are intrinsically connected with serious crime and terrorism. This may also have a negative impact in other aspects of the lives of asylum seekers, as often police records (even if the person is found innocent) are

1221 Meijers Committee, ‘Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac’ (n1194) 3; EDPS, ‘Opinion on the Eurodac proposal of 2009’ (n1082) ¶47; EDPS, ‘Opinion on the Eurodac proposal of 2012’ (n1118) ¶39; Meijers Committee, ‘Note on the Eurodac proposal of 2012’ (n1118) ch 1; UNHCR, ‘An Efficient and Protective Eurodac’ (n1131) 10-11.
1224 House of Lords, ‘Schengen Information System’ (n503) 18.
1225 UNHCR, ‘An Efficient and Protective Eurodac’ (n1131) 10-11.
consulted for potential employment or housing. As a result, asylum seekers may face difficulties with regard to integration.1226

As for the modalities of law enforcement access, I contend that the rules are carefully drafted. The conditions are stricter than the respective rules on law enforcement access to VIS, pointing to the direction that the vulnerable position of asylum seekers was taken into consideration. However, a few points of concern must be raised. The first problem relates to the type of national body that qualifies as a competent authority for the purpose of the Regulation. This is a recurring issue that also emerged in the context of VIS and SIS.1227 The definition of a ‘designated’ authority is insufficient, vague and leaves a large amount of discretion to Member States to designate any authority they consider related to law enforcement. There exists no requirement for prior publication of a list of these bodies in the Official Journal of the EU and no further control at EU level. As for the exclusion of national intelligence authorities, although this is certainly a welcomed development, particularly because in the Commission proposal of 2012 this possibility was not ruled out, the EU does not have competence to legislate on issues of national security. It is therefore unclear how this provision will be enforced.1228

Another recurring issue, already pointed out in the VIS case study, is the definition of serious offences by reference to the EAW Framework Decision. Apart from the points raised in Chapter 3 regarding the beefing up of definitions of terrorist offences,1229 there is a further issue worth noting. As it has been pointed out, despite the fact that in comparison to the VIS, a further explanation of the term ‘serious crime’ is provided, the barrier is relatively low, particularly in those Member States whose criminal law allows potentially long custodial sentences for fairly minor crimes.1230

A particularly worrisome aspect relates to the functioning of the verifying authority. The respective provisions of the Regulation are problematic in several respects. Firstly, the verifying authority is a law enforcement authority which may also form part of the same organisation as the agency seeking access. Though this policy choice may seem to make practical sense, as the verifying authority could perhaps better understand the needs of a criminal investigation, it is likely that the decision regarding the fulfillment of conditions could be biased, particularly if the officials involved are situated within the same organisation and/or the same premises. The multiple references

1226 ibid.
1227 See Chapter 2, Section 5.5.4 and Chapter 3, Section 4.6.
1229 See Chapter 3, Section 4.6
1230 Peers and others (n1069) 437.
to the independence of the verifying authority in reaching their decisions, which are spread throughout the Regulation, albeit necessary, may prove inadequate. This is because once the verifying authority has concluded that the conditions of access have been fulfilled there is no other mechanism prior to the transmission of the request to ensure that this assessment was indeed accurate. The verifying authority merely needs to transmit the request to the National Access Point without mentioning the reasons for the decision. It would have been appropriate to entrust the examination of the conditions for access to a judicial or national supervisory authority, or at least a review of the conditions by these authorities could take place. This would have been in line with the Grand Chamber’s proclamations in *Digital Rights v Ireland*, according to which access to data by the competent national authorities should be made dependent on a prior review carried out by a court or an independent administrative body.\footnote{Digital Rights v Ireland (n326) ¶62.} The sole possibility of controlling the process is *ex post* through supervision by national DPAs, which may take place months or years later. Hence, it could be argued that the current wording of the provisions does not restrict the powers of the verifying authority in an effective manner. This could result in the strict wording of the provisions being ineffective in practice, and asylum seekers’ data processed for law enforcement purposes more systematically than intended.

Moreover, the possibility of consulting Eurodac for law enforcement purposes does not end with the acquisition of refugee status or subsidiary protection. As mentioned above, pursuant to Article 18 of the recast Regulation, the data of beneficiaries of international protection are marked by the Member State which granted protection. This means that for an additional period of three years starting from the date on which the applicant was granted international protection, the data remains at the disposal of designated authorities and Europol. This is a novelty of the Regulation, since under the former regime when an asylum seeker was granted international protection, their data were immediately blocked and no further use of the data could take place.\footnote{Eurodac Regulation, art 12.} Hence, the marking of data is an intermediate stage between the full use of the data of beneficiaries of international protection and the complete blocking of use of this data, which takes place only after the expiration of the three-year period. This change in approach indicates that the cloud of suspicion also covers third-country nationals who have been recognised as particularly vulnerable and in need of protection.

Finally, searches in the database based on latent fingerprints may lead to a high number of possible matches, given the wider range of possible correlations with partial
or fragmentary prints. Furthermore, the rates of error (false matches) could increase, and this could result in adverse consequences for innocent asylum seekers who may be wrongfully implicated in criminal investigations.

4.3 Assessing the re-package of Eurodac as an instrument for ‘wider immigration purposes’

Regrettably, the aforementioned concerns have not resulted in reconsidering the Eurodac legal framework altogether. Quite the contrary; the forthcoming revision testifies that the EU institutions wish to intensify surveillance of movement of all undocumented third-country nationals. In particular, the Eurodac reform has taken place both quantitatively, through the expansion of the scope *ratione personae* and the obligation to register additional categories of data, including sensitive ones, and qualitatively, by detaching Eurodac from its original Dublin context and re-conceptualising it as a multi-purpose tool. In addition to the privacy concerns that are outlined below, it must be noted that it is questionable whether Eurodac can operate as a mixed instrument encompassing both asylum and immigration law prerogatives. Since the UK and Ireland are not full Schengen States, it would be paradoxical to consult a database meant to assist in identifying irregular migrants for the purpose of return, if the latter will take place on the basis of national rules. Be it as it may, the proposed legislation raises serious privacy concerns regarding the generalisation of surveillance, since Member States shall be able to conduct comparisons of fingerprints obtained from irregular migrants at both the external borders and within national territory, within the whole context of the system.

As such, the ‘new Eurodac’ interacts with the right to private life in a variety of ways. Firstly, the additional aims foreseen signify a considerable deviation from the original purpose of the system, which was not foreseen at the time of the collection. It marks an era where once information is collected it can then be used in a multiplicity of contexts, even without prior scrutiny or much justification, even if the individuals concerned have not been informed about it beforehand. This will be the case with the data currently stored on irregular border-crossers who are currently informed about the possibility of their fingerprints to be used solely for Dublin-related purposes. Secondly, in addition to the registration of fingerprints, applicants for international protection and

---

1234 ibid; UNHCR, ‘An Efficient and Protective Eurodac’ (n1131) 5-6.
irregular migrants will also be photographed and their facial image will be recorded in
the system. This process enhances the negative connotations with criminality generated
by fingerprinting and deepens the feeling that the movement of these individuals is
monitored. The vague feeling of surveillance is further exacerbated by four factors: the
expansion of the categories of data stored; the mandatory recording of irregularly
present migrants; the lower minimum age for registration; and the extension of the
retention period, all of which will significantly magnify the size of Eurodac. Consequently,
the revised framework transforms Eurodac from a relatively restricted
database, compared to VIS and the SIS II, into a powerful tool of mass surveillance of
movement, with the aid of which national authorities shall be able to track third-country
nationals whose data are recorded within the EU for as long as they remain on EU
territory. This involves not only irregular migrants, whose movement is monitored with
a view to ‘getting them out’, but also in relation to beneficiaries of international
protection, in which case, surveillance is aimed at confining them to where they belong
territorially. National authorities shall be able, on the basis of a ‘hit’, to recreate
migration routes on an unprecedented scale by processing ‘real-time’ information. Even
the name ‘Eurodac’ will no longer be relevant, as the system will not merely store
fingerprints, but maintain complete files on all individuals found without legal
documents in the EU.

In light of the above, and bearing in mind the magnitude and capabilities of the
foreseen system, the interference with the right of private life must be considered as
particularly serious, which necessarily delimits the margin of discretion enjoyed by the
EU legislature. It must be further recalled that, as mentioned in Chapter 3, this
particularly serious limitation to privacy is provoked primarily for administrative
purposes, related to better implementation of broad immigration purposes.

The additional objectives of the ‘new Eurodac’, namely the ‘control of illegal
immigration’, ‘secondary movements within the Union’ and the ‘identification of
illegally staying third-country nationals’ must be considered as purposes of general
interest of the EU, falling within the auspices of implementing the EU’s return policy
and combating irregular migration. Nevertheless, the proposal does not clearly explain
these purposes, particularly with regard to what constitutes ‘appropriate measures’ apart
from removal and repatriation, or what is the ultimate aim of the Commission. In this
respect, it must be observed that the necessity of revising Eurodac is, at best, extremely
doubtful.1235 As in the case of law enforcement access, the revised proposal has not been
accompanied by an impact assessment as to whether this will actually prevent irregular

---

1235 On this issue see ECRE, ‘ECRE Comments on the Commission proposal to recast the Eurodac
migration and will assist in the identification of irregular migrants, so as to expand the scope of the system beyond its asylum law remits. The sole explanation provided involves the need to collect and store a facial image on top of fingerprints, which is grounded on cases where third-country nationals refuse to undergo the fingerprinting process in an attempt to by-pass the Dublin rules, or due to fear that their personal data will be misused. However, instead of reconfiguring the EU’s asylum policy more broadly, in order to re-construct relations of trust with applicants for international protection, the Commission opted for introducing an additional means of assigning an identity to third-country nationals as an alternative. Furthermore, it has not been explained why it is necessary to expand the process of fingerprinting to irregular residents, whose fingerprinting is already disproportionate (as analysed earlier), or to irregular border-crossers. The lack of definition of irregular border-crossers becomes even more acute in this case, as it may lead to divergent implementation.

Moreover, this expansion seems to disregard the fact that the SIS II already stores alerts on persons who must be refused entry or stay, therefore a mechanism enhancing the implementation of the return policy is already in place. Under the revised regime, irregular migrants could be registered in the system even prior to the issuance of a return decision, thus circumventing the SIS II safeguards, since a third-country national’s information will be recorded in any case, irrespective of any personal circumstances. Consequently, Eurodac will lead to generalised and indiscriminate collection and further processing of personal data of all third-country nationals whose entrance or residence is irregular. The enrolment will even cover minors for the purposes of establishing links with family members in other Member States. In principle, this is a noble purpose; however it must be accompanied by limitations in its use, particularly by a prohibition of consultation for law enforcement purposes and restrictions on the use of the data solely for the purpose of identifying relatives. The undifferentiated treatment of irregular migrants and applicants for international protection disregards the vulnerability of the latter group of individuals, and the particularities of each distinct policy. Another point of concern is that secondary movements within the EU should not be treated in the same way as irregular migration; a refugee may have valid reasons for traveling from a country that does not provide any protection to a Member State where they are safe. With regard to the categories of data collected, it is not evident why the system must store the categories

---

1236 By analogy to S and Marper v UK (n194) ¶124.
1237 Meijers Committee, ‘Note on the reforms of the Dublin Regulation, the Eurodac proposal and the proposal for an EU Asylum Agency (CM1609, 2016).
prescribed, as the underlying rationale seems to be the alignment to other existing databases, which is in principle an irrelevant factor. As for the inclusion of both fingerprints and a facial image, it is astonishing why the requirement to register an additional type of sensitive biometric data has not been accompanied by a revision of the existing rules requiring the enrolment of a full set of fingerprints. Finally, in relation to the retention period of data, it is striking that the proposal persists on the rule requiring the storage of asylum seekers’ personal data for 10 years. The duration of the retention period for irregular migrants is also disproportionate to the aim pursued. According to the Commission, the aim of such collection and storage will be to use this information ‘to assist a Member State to re-document a third-country national for return purposes’. Taking also into account the maximum length of detention for the purposes of return to the country of origin, the five-year retention period seems unreasonably long. Arguments related to the duration of an entry ban or the length of the retention period for other categories of third-country nationals in other databases are irrelevant, as each database functions, in principle, for different purposes, which effectively determine the retention period. A possible alignment seems to serve not the objectives of the database, but rather the underlying and future aim of the Commission to interconnect the different systems.

5. Conclusion

The case of Eurodac is vital in comprehending how consecutive reconfigurations of massive databases raise significant privacy concerns by losing touch with the initial purpose for which the data are collected. In its initial conceptualisation, Eurodac was a rather specific instrument directly linked to the effective application of the Dublin mechanism for the allocation of responsibility for examining an asylum claim. In comparison to the other currently operational systems, it had a limited mandate, as exemplified also by the few categories of personal data stored, and its operation solely on the basis of biometric data. Even so, the operation of Eurodac as an asylum tool raises privacy concerns due to the mandatory collection and storage of biometric information in a large-scale system. Furthermore, emphasis is overly placed on the

1239 Commission, ‘Eurodac proposal of 2016’ (n1003) explanatory memorandum, 3.
effectiveness of biometric information without due concern on the effect of false matches to persons who are wrongly identified. In addition, the mere existence of Eurodac is called into question as the Dublin system in itself is malfunctioning, not least due to highly divergent conditions experienced in different Member States. The extension to irregular residents is another disproportionate feature of the system, which, however, paved the way for the extension of Eurodac to pursue wider immigration aims.

The new law enforcement functionality of the database affects the position of asylum seekers in multiple ways: their fingerprints will be collected and stored for a double purpose that deviates from the original objective for which the database was set up. Furthermore, this approach distinguishes asylum seekers from other categories of third-country nationals, which may lead to increased stigmatisation. Whereas the Parliament managed to secure strict conditions of access and improve the Commission’s proposal in numerous respects, it has been demonstrated that a number of issues remain problematic. Importantly, the necessity of law enforcement access to asylum seekers’ data is rather ambiguous. A comprehensive evaluation of the insufficiency of existing means of information exchange, and a holistic, up-to-date and clear justification of how asylum-seekers’ data would be beneficial to Member States and Europol should have taken place before the adoption of the Regulation. Indeed, it appears that the Member States lobbying for law enforcement access to Eurodac already stored asylum seekers’ data in their national AFIS. As a result, under Prüm they already share asylum seekers’ information with other Member States. This design of the national AFIS, which is rather disturbing in itself, because it equates criminals’ and asylum seekers’ data, was part of the justification proposed by the Commission when explaining the necessity of the measure granting access to law enforcement agencies. Furthermore, the loopholes found in certain provisions, the obscure justifications proposed by the Commission and the lack of clear, non-fragmentary evidence point to a link between asylum seekers and criminality that is still apparent.

The recent Commission proposal to revise the Eurodac rules emerged less than a year after the recast Regulation came into effect, and even before an evaluation of the Commission scheduled for 2018. It is indicatory of a disturbing conflation between immigration and asylum imperatives and denotes a disregard on the specified purpose for which the data is collected. By stretching the personal, material and temporal scope of Eurodac, the system is transformed from the ‘ugly duckling’ of databases, which was fairly restricted in capacity, to a fully-fledged, powerful, investigatory tool. As such, it will enable the tracking of movements of the irregular migrants and applicants for international protection either when they move in search of asylum in another Member State or when they change location to find better living conditions or work. To that end,
Eurodac is destined to store, in a generalised and indiscriminate manner, personal information, including two categories of sensitive data, of all irregular migrants and applicants for international protection. This considerable expansion has not been accompanied by sufficient explanations regarding its necessity, particularly since there is no comprehensive information on the magnitude of the problem of irregular migration and the existence of other mechanisms already in place. In this respect, the mandatory registration must be seen as a means to compile statistical information on this issue, including the migratory routes preferred by third-country nationals, without clear indications of what is the ultimate aim pursued. This is a clearly disproportionate policy choice. Additionally, two categories of sensitive data will be centrally stored, which will also be accessed by law enforcement authorities and Europol, thus further enhancing the risk of stigmatisation, as it will be easier for irregular migrants to be identified as opposed to other groups of individuals who are not catalogued at EU level.

The recent Eurodac proposal is not the sole instrument currently under negotiations. The wide complex of centralised information systems will soon be supplemented by another huge database, aimed at ‘filling the gap’ generated by the lack of information on visa exempt third-country nationals who wish to enter the Schengen territory as tourists. Hence, the EES – the ‘little’ sibling of VIS – will constitute the largest information system surveying the entry in and exit from the Schengen territory of more than 50,000,000 travellers. The privacy concerns it entails are worth exploring.
CHAPTER 5. ‘Mind the (Information) Gap’: The Normalisation of Surveillance of Movement via the Entry/Exit System (EES)

‘A situation is developing in which information about not just suspected criminals or criminal deeds is being collected, but simply everyday behaviour.’

1. Introduction

In Chapters 2-4, I analysed the three currently operational databases aimed at monitoring the movement of various categories of third-country nationals, namely irregular migrants, short-stay travellers subject to visa requirements and applicants for international protection. Although these systems create a rather comprehensive network of information exchange, there is a large group of third-country nationals who are currently unmonitored, namely foreign visitors originating from countries whose nationals are not subject to visa requirements. In light of this alleged information ‘gap’, the Commission presented three legislative proposals on 28 February 2013, forming the so-called ‘Smart Borders’ package. The package included a proposal to establish a new large-scale centralised database, the Entry/Exit System (EES), designed to record and monitor the entry and exit of all third-country nationals crossing the Schengen external border. It was accompanied by a proposal to set up a Registered Traveller Programme (RTP) for the facilitation of border crossing for pre-screened trusted travellers. As for the third proposal, it prescribed amendments to the Schengen Borders Code (SBC) stemming from the reforms that the two other proposed


1244 See n848.
instruments would entail.\textsuperscript{1245} There proposals, which they take their cue from measures conceived in the US, has elicited considerable debate, leading the Commission to withdraw the package. On 6 April 2016 the Commission re-tabled its EES proposal,\textsuperscript{1246} accompanied by a proposal concerning changes to the SBC.\textsuperscript{1247}

Whereas the RTP is discussed in Chapter 6, this Chapter is devoted to the privacy concerns raised by the future establishment of the EES. Firstly, I briefly outline the origins of the EES, both in the US and in the EU. Then, I set out the main provisions of the two Commission proposals, followed by an analysis of the privacy concerns.

2. The story behind the EES proposals

2.1 ‘Born in the USA’: The origins of the EES

The background of the EES must be discussed in combination with the actions undertaken by the US Government in the wake of the 9/11 events. As observed in Chapter 2, the focus on implementing a securitised model of immigration control – rebranded as border security – was grounded on the collection and exchange of massive amounts of information, including sensitive data, with a view to identifying dangerous individuals not only among immigrants, but among travellers more broadly.\textsuperscript{1248} Nevertheless, the vision of developing ‘smart borders’ on the one hand, and the idea to establish a system recording the entry and exit of non-US nationals on the other, did not emerge within the same context. Initially, the concept of ‘smart borders’ first came up in relation to the US-Mexico border, but is customarily associated with the ‘Action Plan for Creating a Secure and Smart Border’ with Canada in December 2001.\textsuperscript{1249} The Action Plan accompanied a Declaration between the two countries committing their border


\textsuperscript{1246} See n982.


\textsuperscript{1248} Mitsilegas, ‘Immigration Control in an Era of Globalization’ (n6) 12.

\textsuperscript{1249} Karine Côté-Boucher, ‘The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada’s Smart Border’ (2008) 5(2) Surveillance & Society 142.
agencies to combat terrorist activity and ensuring public and economic security. The National Strategy for Homeland Security of 2002 called for the establishment of a ‘border of the future’ more broadly, whereby ‘a layered management system’ would enable greater visibility of vehicles, persons and goods coming to and departing from the US. Emphasis was placed on screening and verifying the security of people well before they would reach the US territory, via the categorisation of populations into degrees of risk.

One of the ways in which this would be achieved would be through the development of a ‘statutorily required entry-exit system to record the arrival and departure of foreign visitors and guests’. Indeed as early as 1996 the Congress mandated the setting up of such a system, but concerns about congestion at border crossings delayed its implementation until 2001. Following the attacks, a series of legislative acts mandated the swift implementation of the entry-exit system, with the Enhanced Border Security and Visa Entry Reform Act of 2001 adding requirements regarding its interoperability with law enforcement agencies. In January 2004, the Department for Homeland Security (DHS) inaugurated the US-VISIT Program (United States Visitor and Immigrant Status Indicator Technology), which since 2013 is known as OBIM (Office of Biometric Identity Management). Its aim is ‘to enhance the security of US citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the US immigration system, and protect the privacy of visitors to the United States’. It is designed to control and monitor the movement of foreign visitors by enabling analyses of the data at four separate stages: before entry (e.g. by refusing to

---

1253 Amoore, (n18) 339.
1255 These were: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56, s 414; Enhanced Border Security and Visa Entry Reform Act of 2002, Public Law 107-173, s 302; The Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, s 7208.
1257 For an overview see Amoore (n18).
grant a visa); upon entry (e.g. verification of identity); during the stay (e.g. information on extension of stay); and upon exit (e.g. verification of departure).\textsuperscript{1259}

Since January 2009, the pool of persons subject to surveillance comprises practically all foreign nationals visiting the US, including lawful permanent residents. As Epstein has rightly noted:

\begin{quote}
\textquote{[t]he US VISIT Program now applies to all foreign bodies, not merely those that have been identified as potentially \textquote{risky} or even \textquote{guilty} […]. In the new border protection practices, each visitor to the US features as a foreign body tagged with an individual calculated level of risk.'}
\end{quote}

Although it initially operated on the basis of two fingerprints alongside biographic information, including entry data, its processing capabilities have been expanded to a full set of fingerprints and photographs.\textsuperscript{1260} The US-VISIT/OBIM includes the interfacing and integration of over twenty existing systems,\textsuperscript{1261} including ADIS (Arrival and Departure Information System), which tracks and matches arrival and departure records for the purpose of identifying potential overstays and IDENT (Automated Biometric Identification System), which stores foreigners’ biometrics. These databases are used to profile and encode people in terms of risk, and checking ‘hits’ against \textquote{inter alia} known and suspected terrorists, criminals and immigration violators.\textsuperscript{1262} Furthermore, the data are shared with numerous government bodies entrusted with immigration, border control, law enforcement, defence and intelligence activities, as well as with foreign governments, including Canada, Australia, and the UK. In effect, the US-VISIT/OBIM form part of a more complex system and constitutes more than just a tool for collecting and organising visitors’ pictures and fingerprints. Rather, it is designed to amalgamate information from these databases through risk assessments and make judgments in relation to both immigration and crime control. In this context, information collected in one part of the network may be used for entirely different purposes by another part of the network.\textsuperscript{1263}

At the time of writing, the matching of entry and exit records is not possible, as the biometric exit capability is still under development, which, in turn, nullifies the

\textsuperscript{1261} Ortiz and others (n1256) 46-7.
\textsuperscript{1262} Amoore (n18) 340.
\textsuperscript{1263} Ortiz and others (n1256) 34.
system’s function to identify potential overstays.\textsuperscript{1264} Whereas the Congress has been pushing towards the insertion of biometrics, the implementation of the technology is lagging behind, because of the significant costs, manpower and the scope of the matter given the high number of exit points in the US territory. A primary point of concern has been the risk that the methods of collecting biometric data will disrupt the flow of travellers, both at land and air borders.\textsuperscript{1265} Other commentators have referred to the infallible character of biometric data\textsuperscript{1266} and the ‘enormous potential for error’ occurred through the processing of data, which may lead to deportation or detention without clear rules for judicial review.\textsuperscript{1267} The GAO has called for the conduct of an evaluation, including the added value of collecting biometrics in addition to alphanumeric data.\textsuperscript{1268} Furthermore, it has been reported that the US-VISIT Program contained significant information security weaknesses,\textsuperscript{1269} which question the adequate protection of individuals given the wide range of authorities consulting the data.\textsuperscript{1270} With regard to specific parameters of the system, calls have been made for revisiting access privileges by allowing access solely to those agencies that require the information as a necessity and for uses for which it was originally collected, and the need to conduct impact assessments prior to extending the functionalities of the system.\textsuperscript{1271}


\textsuperscript{1265} GAO, ‘Actions Needed by DHS to Address Long- Standing Challenges in Planning for a Biometric Exit System’ (GAO-16-358T, 20.01.2016) 6-7.


\textsuperscript{1268} GAO, ‘Actions Needed by DHS’ (n1265) 2016.


\textsuperscript{1270} EPIC, ‘Biometric Data Collection at the Ports of Entry’ (n1260).

2.2 From the VIS to the EES

At EU level, the first traces of the EES are found in a Council Document of October 2001 calling for the extension of Article 96 CISA alerts, so as to enable checks on whether third-country nationals to whom a visa was issued and expired had actually left the Schengen zone. If not, an alert in SIS would be registered.\textsuperscript{1272} Although that proposal was not pursued further, the idea of monitoring the movement of all third-country nationals featured in the Hague Programme of 2004 as forming part a ‘continuum of security measures’ which ‘are also of importance for the prevention and control of crime, in particular terrorism’.\textsuperscript{1273}

As explained in Chapter 3, that momentum was high for the establishment of the VIS. However, mirroring the US approach, the feasibility study carried out in relation to the VIS scrutinised the development of the EES – solely for visa holders – as a policy option.\textsuperscript{1274} That alternative was rejected on financial and fundamental rights grounds and concerns were also expressed about the timings for border crossing and the collection of biometric data.\textsuperscript{1275} Having agreed on the creation of the VIS, the idea of an EES momentarily remained on the backburner, until the Commission identified in 2008 three gaps in information exchange: the lack of benefits for frequent \textit{bona fide} travellers;\textsuperscript{1276} the lack of enhanced checks on third-country nationals who are not subject to visa requirements;\textsuperscript{1277} and incomplete monitoring of entry and exit of third-country nationals. In view of these shortcomings, the Commission found that ‘the technical feasibility of an entry/exit system has in the meantime improved due to the development of the VIS’. The EES was thus reframed as a flanking measure to the VIS, even though it was originally conceived as its alternative.\textsuperscript{1278} Such a system would not be extended to EU citizens ‘as this would be incompatible with the principle of free movement’.\textsuperscript{1279} In compensation for the additional time that would be required for border crossings, the system would be complemented by a programme for simplified travel of \textit{bona fide} travellers.\textsuperscript{1280}

\begin{thebibliography}{99}

\bibitem{1272} See n519.
\bibitem{1273} The Hague Programme (n7) 14.
\bibitem{1274} EPEC, ‘Study for the Extended Impact Assessment’ (n773) 25.
\bibitem{1275} ibid 34, 47.
\bibitem{1276} Commission, ‘Improved effectiveness’ (n780).
\bibitem{1277} ibid 6. Notably this shortcoming was identified ‘by the internal security and intelligence communities’.
\bibitem{1279} Commission, ‘Improved effectiveness’ (n780) 9.
\bibitem{1280} ibid.
\end{thebibliography}
Preparatory work and discussions have taken more than eight years, within which time the EES featured in a series of policy documents. A sneak-peak of the envisaged system was put forward by the Commission in a Communication of 2008, accompanied by an Impact Assessment, which was drafted on the basis of two studies. The Commission focused on the problem of overstayers, deemed as presenting ‘by far the biggest category of illegal immigrants in the EU’, and called for the establishment of a truly integrated border management, an objective comprising of two sub-aims; the enhancement of security and the facilitation of travel for third-country nationals. To that end, in addition to the aforementioned initiatives, the Commission briefly mentioned that it would examine the possibility of introducing an Electronic System of Travel Authorisation (ESTA) to pre-screen third-country nationals, irrespective of whether they were subject to a visa regime, in order to verify that they fulfill the entry conditions before travelling to the EU. In wait of a proposal by 2010, the then Swedish Presidency issued a questionnaire, in which the objectives of the EES revolved around the phenomenon of overstayers.

The idea for establishing a new database was endorsed by the Stockholm Programme, noting however that ‘the introduction of the system at land borders deserves special attention and the implications to infrastructure and border lines should be analysed before implementation’. Another study was commissioned, leading to the European Council meeting of June 2011 calling for the rapid development of the

1284 Commission, ‘Preparatory Study to inform an Impact Assessment in relation to the creation of an automated entry/exit system at the external borders of the EU and the introduction of a border crossing scheme for bona fide travellers (‘Registered Traveller Programme’)’ (GHK, 2007); ‘Entry-Exit Feasibility Study’ (UNISYS, 2008).
1285 A study was released in this respect. See Commission, ‘Policy Study on an EU Electronic System for Travel Authorisation’ (PwC, 2011).
1286 Council, Document 12251/08 (28.07.2008). Nationals delegations’ views differed significantly. The inclusion of biometric identifiers was widely agreed, but certain Member States raised proportionality concerns. Most delegations favoured a five-year retention period, but it was suggested that different retention periods could be foreseen depending on whether the third-country national left the Schengen territory or is a visa holder. See Council, Documents 13403/08 (24.09.2008) and its additions; 14334/08 (16.10.2008); 15630/08 (01.12.2008).
1287 Stockholm Programme (n606). Further questionnaires circulated. See Council, Documents 7226/1/09 (18.03.2009); 8552/08 (21.04.2009); 13267/09 (22.09.2009).
package. A key factor for renewing interest was the increased number of people traveling to Europe in the aftermath of the Arab Spring. Instead of a proposal, the Commission published a Communication on smart borders as a response to the EDPS’ opinion that the setting up of a new system should meet the requirement of necessity. Acknowledging that the mere monitoring of authorised entries of registered travellers is not a justification for setting up a system that would put all travellers under surveillance, the Communication suggested setting up the database in two stages; under the first phase, the system would enroll alphanumeric data only. Under the second phase, and after the first evaluation results, biometric identifiers could be activated. Law enforcement access to the EES was marginalised, with the Commission stating that such possibility could exist in cases clearly defined by the future EU legislation.

Unsurprisingly, that Communication was met with skepticism by Member States, which had widely agreed that biometrics should be captured from the beginning of the operation of the database and desired the inclusion of a law enforcement purpose within its mandate. Against this background, on 28 February 2013, the Commission presented its proposals accompanied by an Impact Assessment. Following the release, a two-speed process within EU institutions took place. Although the Council found that numerous aspects were nuanced, it immediately began scrutinising the proposal, with the national delegations pressing towards significant changes in the purpose and operation of the system. As for the Parliament, a Parliament Official mentioned that already at an early stage it was evident that the EES proposal was ‘unworkable’. In effect, no resolution was issued.

1293 Commission, ‘Smart Borders’ (n1291) 9.
1294 ibid 12.
1296 Commission, ‘Staff Working Document – Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union’ SWD(2013) 47 final (Impact Assessment of 2013). The Commission submits that 13 Member States currently deploy their own NEES. The national systems perform on the basis of alphanumeric data, which are stored for periods ranging between five and 25 years and may be processed for multiple purposes including law enforcement and risk analysis. See Commission, ‘Smart Borders’ (n1291) 6.
1297 For a consolidated approach see Council, Document 8418/14 (15.04.2014).
1298 Informal discussion with a Parliament Officer (Brussels, November 2014).
In view of the voiced criticism, the Commission requested the conduct of a new study accompanied by a one-year pilot project to be entrusted to eu-LISA, both comprising the so-called ‘proof of concept’. In December 2014, it was announced that the package would be withdrawn. Extensive consultations and discussions continued in quiet throughout 2015, and a joint police operation named AMBERLIGHT was launched. The latter was an intelligence-gathering exercise to illuminate whether third-country nationals depart from the Member States where they had overstayed or from another one in order to conceal the violation, and which visas from which Member States are mostly detected.

In this context, on 6 April 2016, the Commission presented its amended proposal partly justified by the growing emphasis placed on visa liberalisation dialogues with countries in the Western Balkans and along the Eastern and South-Eastern borders, which led to an increasing proportion of visa-exempt travellers to the EU. Consequently, the liberal approach towards the abolition of visa requirements has been coupled by security concerns resulting in the EES having become a flanking measure of the EU’s visa policy. In view of the background work that has already taken place in between the two proposals, and the current highly securitised landscape under the pressure of terrorist attacks, negotiations are expected to move very fast with a view to the adoption of the EES Regulation by the end of 2016.

---


1300 See n706.


1302 For the steps of the process see Council, Documents 17127/13 (11.12.2013); 5193/14 (10.01.2014); 5386/14 (17.01.2014); 6040/14 (03.02.2014); 5828/14 (04.02.2014); 6993/14 (27.02.2014); 15922/14 (27.11.2014); 17060/14 (19.12.2014).


1305 See n982.

1306 ibid 6.
3. Towards the establishment of a ‘Schengen Hotel’:
Mapping the Commission proposals

With the exception of third-country nationals residing in border areas of neighbouring countries, all third-country nationals must undergo thorough checks in order to cross the EU external border. The duration of this procedure varies depending on the type of border (sea, land, air); according to FRONTEX, border guards typically devote 12 seconds per third-country national to reach a decision on admissions. Overall, the Commission estimates that the average time for a border check for visa holders, in entry at the land border, is 2’17”, and for visa exempt nationals 1’12”. On exit, the average time is 1’34”, and for visa exempt nationals 58”. As for the air borders, on entry the respective timings are 1’44” and 1’03”, and on exit 1’11” and 52” respectively.

3.1 The proposal of 2013

3.1.1 Main characteristics of the proposed EES

As mentioned earlier, the idea behind the EES is to record the entries and exits of third-country nationals admitted for short stay and subject to thorough checks pursuant to the SBC, and to substitute the ink-on-paper stamping of passports with digital records. In particular, upon entry, the border guard would check whether the third-country national concerned is registered in the EES and if not an individual file would be created, including a series of information. Each time the visitor would enter and exit the Schengen area the system would register data on the date, time and the Member State of entry or exit, as well as the maximum term of authorised stay in accordance with the Schengen Borders Code. An important feature of the database was

---

1308 SBC, art 7.
1310 Commission, ‘Impact Assessment of 2013’ (n1296) 64.
1311 Commission, ‘EES proposal of 2013’ (n1242) art 3, which exempts: a) members of the family of an EU citizen to whom Directive 2004/38/EC applies who hold a residence card; b) members of the family of nationals of third countries enjoying the right of free movement under EU law who hold a residence card; c) holders of residence permits; d) nationals of Andorra, Monaco and San Marino.
the generation of automated alerts in cases when the system would not have information on the exit of a person upon expiration of the prescribed period of lawful stay.\(^{1312}\)

The system was justified on immigration policy grounds and its aims were divided into primary and secondary ones. According to Article 4 of that proposal, the primary aim of the EES would be to improve:

‘[t]he management of the external borders and the fight against irregular immigration, the implementation of the integrated border management policy, the cooperation and consultation between border and immigration authorities by providing access by Member States to the information of the time and place of the entry and exit of third country nationals at the external borders and facilitating decisions relating thereto’.

In addition, five sub-objectives were identified:

a) Enhancing external border checks and combating irregular immigration;
b) Calculation and monitoring of the duration of the authorised stay of third-country nationals admitted for a short-stay;
c) Assistance in the identification of irregular migrants;
d) Enabling the identification of overstayers and taking appropriate measures; and
e) Gathering statistics on the entries and exits of third-country nationals for the purpose of analysis.

In this ‘patchwork’ approach, similar to the one endorsed in relation to the VIS, four main aims can be discerned: a) to improve the efficiency of checks at external borders; b) to combat the problem of overstayers; c) evidence-based policy making by gathering reliable statistics; and d) easier returns, by allowing national authorities to identify persons who have destroyed their travel documents.\(^{1313}\)

Worryingly, the Impact Assessment accompanying the proposal of 2013 identified the contribution to the fight against terrorism and other serious crime and the promotion of a high level of internal security as an objective pursued by the system, even though law enforcement was not envisaged.\(^{1314}\)

In this framework, the EES would register no less than 36 categories of data, including biographic details and information on the travel document, visa and RTP status where applicable. As already mentioned, details on the place, date and Member State of entry and exit, as well as the calculation of the number of days of the authorised

\(^{1312}\) ibid art 10.
\(^{1313}\) ibid.
\(^{1314}\) Commission, ‘Impact Assessment of 2013’ (n1296) 25.
stay would be recorded. As for the inclusion of biometrics, the Commission maintained the view regarding a phased integration of fingerprints three years after the system would become operational. Certain delegations favoured the inclusion of 10 fingerprints, but others took a pragmatic approach requesting a reduction in the number of fingerprints taken in view of the long queues to be anticipated at the borders. The storage period depended on whether the travellers were ‘bona fide’ or overstayers. According to Article 20, in ‘ordinary’ cases, the retention period would be 181 days at most. Each individual file with the linked entry/exit record(s) would be stored for a maximum of 91 days after the last exit record, if there would be no entry record within 90 days following the last exit record. In case of overstayers, data would be stored for a period of five years following the last day of the authorised stay. Almost unanimously, all Member States called for a longer retention period, with a large number of them calling for a unified retention period of five years. As for rules on transfers of data, individual rights and supervision, these matched the ones in the VIS Regulation.

3.1.2 The ‘elephant in the room’: Law enforcement access to EES data

Recital 23 of the proposal stipulated that:

'[t]he conditions of giving access to the data stored in the system for law enforcement purposes and to third countries, and of retaining the data for different periods should further be evaluated in order to assess whether and, if so, how the system can contribute most effectively in the fight against terrorist offences and other serious criminal offences. Given the high number of personal data contained in the EES and the need to fully respect the private life of individuals whose personal data are processed in the EES, this evaluation should take place three years after the start of operations and take into consideration the results of the implementation of the VIS’.

Although, apparently, access would be regulated at a later stage, Recital 11 further stated that ‘the technical development of the system should provide for the possibility of

---

1315 Commission, ‘EES proposal of 2013’ (n1242) arts 11-4.
1316 ibid art 12.
1318 Council, Document 11143/13 (20.06.2013) 7.
1319 Council, Documents 16038/13 (18.11.2013); 11670/14 (15.07.2014).
access to the system for law enforcement purpose should this Regulation be amended in the future to allow for such access’.

Member States were clearly dissatisfied with these provisions. As early as in May 2013, no less than 20 States expressed their wish to grant law enforcement authorities access to the EES data from the outset of its operations. The Commission noted with concern the lack of proportionality between, on the one hand, the data collected and stored in the EES and, on the other hand, the usefulness of EES data in combating serious crime due to difficulties in ascertaining the rate of success on the basis of using such data. Therefore, Member States were invited to submit examples from the operation of domestic entry/exit systems. Furthermore, it was made clear that significant costs for setting up the EES did not justify expanding its objectives.

Notwithstanding the Commission warnings, by mid-2014, it was evident that Member States were eager to grant law enforcement from the outset of operations. Member States continued to brainstorm on the matter by focusing on which model should be followed when developing the database – the VIS or the Eurodac one. Most delegations favoured using the VIS as an example, since it ‘is much closer to EES than the Eurodac, which was built on a different legal framework’. It was submitted that law enforcement access would ‘complement the access already granted’. Therefore, the issue was not considered independently, but was heavily influenced by other operational databases.

Opening up the EES to the police influenced two controversial aspects of the proposal, namely the issue of whether to include biometric data and the duration of the retention period. With regard to biometrics, according to the Commission:

‘[t]he use of biometric data, and more specifically fingerprints, would substantially increase the added value of the entry/exit data in establishing the identity of a person who is suspected of a crime or a crime victim such as victim of trafficking in human beings’.

Furthermore, the then Greek Presidency mentioned that ‘for law enforcement purposes, it seems that the most important data to have access to are the fingerprints, because they

---

1321 Council, Document 9863/13 (28.05.2013) 5.
1322 ibid.
1323 Council, Document 10720/13 (07.06.2013) 4.
1324 Council, Document 6626/4/14 (15.05.2014).
1325 Council, Document 11337/14 (08.07.2014) 2-3. Compare with Council, Document 10720/14 (12.06.2014) where the Eurodac model was favoured.
would enable identifying a suspect.'\textsuperscript{1328} As for the retention period, the French delegation took the view that:

‘[i]t would be preferable to have a retention period of significantly longer than the 181 days currently proposed for third-country nationals having respected their authorized length of stay, in order to allow law enforcement authorities, when their investigations require it, to trace a posteriori the movements of individuals wanted not due to their residence status but for security reasons.’\textsuperscript{1329}

This phenomenon, whereby this ancillary objective of the EES compromises certain parameters of the system that would otherwise be determined solely on the basis of immigration control considerations, could be termed as the ‘vertical spillover effect’ of law enforcement access. Criminalisation of foreign travellers takes place in a diverse manner, as security considerations go beyond the mere issue of whether police authorities could consult EES data. Coupled with the premature references in the proposal which suggest that law enforcement access was almost taken for granted, the database already at this stage was getting ‘prepared’ for being used in criminal investigations. To that end, other sensitive features were directly affected and pre-fixed in order to accommodate this functionality, thus giving in to the risk that it ‘obscures the discussion on the desired form’ of the database.\textsuperscript{1330} Such efforts further blur the boundaries between immigration-related objectives and criminal law ones, leading to a transformation of the EES into a criminal investigation tool through the back door.

\textbf{3.2 The proposal of 2016 }

Discussions continued until late 2015 with a view to ‘guiding’, or even pre-empting, the Commission in preparing its proposal.\textsuperscript{1331} Under the amended proposal of 2016, the EES will expand surveillance of movement to almost all non-EU travellers, whose personal data, including biometrics, will be captured, stored and further processed \textit{en masse}, including for purposes pertaining to criminal law.\textsuperscript{1332} Furthermore,
stamping will be replaced by the creation of entry/exit records.\textsuperscript{1333} The Commission envisages the system structured on the basis of the VIS model,\textsuperscript{1334} with which it will be interoperable by way of a direct communication channel for specific purposes,\textsuperscript{1335} and allowing the use of existing NEESs.

Due to its expanded purposes, the revised proposal is legally based on Articles 77(2)(b) and (d) TFEU regarding measures on external border checks and Articles 87(2)(a) and 88(2)(a), so as to allow access for criminal law purposes by national law enforcement authorities and Europol. The EES constitutes a development on the Schengen acquis, therefore Denmark will have to decide whether they would opt in to the Regulation, whereas the UK and Ireland will not be able to participate. Associated Schengen States (Switzerland, Norway, Iceland and Liechtenstein) will form part of the system. As for those Member States that do not apply the Schengen acquis in full (Cyprus, Romania, Bulgaria and Croatia), the EES will apply from the date on which the controls at the internal borders are lifted.

The main features of the proposed EES are as follows:

\textbf{3.2.1 Purpose}

The stated objectives have undergone significant reform in comparison to the original proposal. The EES is now envisaged as a powerful ‘all-rounder’ system, pursuing no less than 12 purposes:

\begin{itemize}
  \item[a)] Enhance the efficiency of border controls by calculating and monitoring the duration of unauthorised stay at entry and exit of third-country nationals;
  \item[b)] Assist in the identification of any person irregularly present;
  \item[c)] Allow the identification and detection of overstayers, and enable competent national authorities to ‘take appropriate measures including to increase the possibilities for return’;
  \item[d)] Allow for electronically checking refusals of entry in the EES;
  \item[e)] Free up border control resources from performing checks that can be automated and enable better focus on assessing third-country nationals;
  \item[f)] Enable consulates to have access to information on the lawful use of previous visas;
\end{itemize}

\textsuperscript{1333} For an analysis of its consequences see Chapter 6, Section 4.
\textsuperscript{1334} Commission, ‘EES proposal of 2016’ (n982) art 6.
\textsuperscript{1335} ibid art 7(2).
g) Inform third-country nationals on the duration of their authorised stay;

h) Gather statistics to improve the assessment of the risk of overstays and to support evidence-based migration policy;

i) Combat identity fraud;

j) Contribute to the prevention, detection and investigation of terrorist offences and other serious crimes;

k) Enable the identification and apprehension of terrorists, criminal suspects or victims crossing the external borders; and

l) Enable the generating of information on travel histories on the aforementioned persons.

The majority of these purposes are broadly related to three categories of challenges: a) addressing border check delays and improving quality of border checks for third-country nationals in view of growing passenger flows;\textsuperscript{1336} b) ensuring systematic and reliable identification of overstayers;\textsuperscript{1337} and c) reinforcing internal security and the fight against terrorism and serious crime,\textsuperscript{1338} which is considered as an ancillary objective. However, it must be noted that the inclusion of certain objectives, namely those under (d), (e) and (g), is problematic, as they seem to be functions of the EES, rather than fully-fledged purposes. Furthermore, it is unclear what the primary objective of the EES is. The confusion becomes greater since Recital 9 of the proposal mentions that the objective of the EES would be ‘improving the management of external borders, preventing irregular immigration and facilitating the management of migration flows’. At the time of writing the Council has already suggested a revision by removing the purpose under (k) and adding another purpose, namely the support in ‘operating their national facilitation programmes, including the examination and decision on applications’.\textsuperscript{1339}

\textbf{3.2.2 Personal scope}

In terms of the scope \textit{ratione personae}, the proposed Regulation covers third-country nationals admitted for short stay, or on the basis of a touring visa, in the territory of the Member States who are subject to border checks in accordance with the

\textsuperscript{1336} By 2025, 887 million border crossing points will take place of which $\frac{1}{3}$ are expected to be performed by third-country nationals travelling to Schengen countries for a short-term visit. See ibid 2. Purposes under a), d), e), g) are included therein.

\textsuperscript{1337} Purposes under b), c) and h) are included therein.

\textsuperscript{1338} Purposes under j), k) and l) are included therein.

\textsuperscript{1339} Council, Document 10880/16 (06.07.2016).
SBC. The categories of exempted persons to which the EES will be inapplicable have been amended, albeit to a limited extent, to explicitly exclude persons who are admitted to the EU on the basis of long-stay visas. The list prescribed by the Commission includes:

a) Family members of EU citizens to whom the Citizens Directive applies and who hold a residence card;
b) Family members of third-country nationals enjoying the right of free movement under EU law who hold a residence card;\textsuperscript{1340}
c) Holders of residence permits;
d) Holders of long-stay visas;
e) Nationals of Andorra, Monaco and San Marino; and
f) Persons or categories exempt from, or benefiting from, facilitation of border crossing.\textsuperscript{1341}

Therefore, the EES is not aimed at controlling the mobility of EU nationals. This does not mean that there have not been attempts to expand the reach of the system to monitor all border crossings. In the name of modernising checks, but essentially prompted by the desire to step up counter-terrorism efforts, France has suggested ‘broadening the scope of the “Smart Borders” package for all travellers, also including European nationals’.\textsuperscript{1342} Such extension would effectively mean systematic verification of travel documents, systematic verification of biometric data available in travel documents (taking place as second line of checks), registration of biometrics data, and registration of the most recent entry and exit in a specific log.\textsuperscript{1343} Controversial as it may be, this possibility has not been entirely ruled out for future endeavours, with the Council Legal Service requesting further details in order to start debating on this suggestion.\textsuperscript{1344}

\textsuperscript{1340} For family members this exemption applies even if they do not accompany or join the EU citizen or a third-country nationals enjoy freedom of movement. Commission, ‘EES proposal of 2016’ (n982) art 2(3) second indent.

\textsuperscript{1341} In effect, beneficiaries of local border traffic regime are exempted from the EES.

\textsuperscript{1342} Council, Document 11272/15 (25.09.2015) 3.

\textsuperscript{1343} ibid 5.

\textsuperscript{1344} Council, Document 13193/15 (17.11.2015) 8. The EDPS refers to a letter written to the European Council of October 2015, where it is stated that ‘such technical solutions could also be explored for EU citizens, to address security challenges’. See Giovanni Buttarelli, ‘A Data Protection Perspective on the Smart Border Package – Focusing on the Possibility of Law Enforcement Authorities’ Access to Border Data’ (2015) 3.
### 3.2.3 Enrolment in the EES and use of collected data

Border guards will be obliged to check whether an individual file has already been created in respect of each visitor, and if so, an entry/exit record will be inserted or, where applicable, a refusal of entry record. Otherwise, an individual file will be created comprising of a set of data, the volume of which has been significantly reduced from 36 to 26 elements. In particular, in relation to visa holders, upon entry the EES will store the following data: name, date of birth, nationality; sex; details on travel document and visa; the number of entries and the authorised period of stay; and a facial image. On each entry and exit, the system will record the data and time of entry and exit and the border crossing point. Furthermore, with regard to persons exempt from visa obligations, in addition to the aforementioned information, and with the exception of visa-related data, four fingerprints from the right hand will also be inserted. Therefore, the Commission dropped the requirement of full fingerprinting and proposes a combination of four fingerprints and the facial image introduced from the outset of operations. Mirroring the VIS rules, the EES will not record the fingerprints of persons below the age of 12. Where legal or factual reasons for no fingerprint registration exist, these will be indicated in the system. The registration of persons who have been refused entry pursuant to Article 14 SBC is a novelty of the amended proposal. In this respect, on top of the data recorded as set out above, the EES will record the refusal of entry by adding the following data: the date and time of refusal of entry; the border crossing point and the authority that refused the entry; and the reason corresponding to the reason(s) of entry. The files will be stored for a period of five years starting from the date of the exit record, the refusal of entry record or the last day of the authorised stay. In the case of non-EU family members of EU citizens falling within the scope of the EES, records will be stored for a maximum period of one year after the last exit. Advance erasure is prescribed in cases when a person acquires the

---

1345 Commission, ‘EES proposal of 2016’ (n982) art 16.
1347 Commission, ‘EES proposal of 2016’ (n982) art 14. On entry the authority that authorised entry will also recorded.
1348 ibid art 15(1).
1349 See Chapter 3, Section 3.2.2.
1351 ibid art 15(3).
1352 ibid art 16.
1353 ibid art 31.
1354 ibid art 31(4).
nationality of a Member State or becomes covered by the exceptions to EES monitoring.\textsuperscript{1355}

Overall, the system will be used by a wide range of competent national authorities entrusted with border checks and visa and immigration control.\textsuperscript{1356} As in the previous cases, these will be designated at the national level and a list of those agencies will be published in the \textit{Official Journal of the EU}, including any future amendments.\textsuperscript{1357} The processing of personal data within the EES is subject to two important safeguards; access must be limited to the extent needed for the performance of the tasks in accordance with the purpose, and proportionate to the objective pursued.\textsuperscript{1358} Furthermore, each competent authority must ensure that the use of the EES is necessary, appropriate and proportionate.\textsuperscript{1359} In particular, border guards will access the EES to verify the identity of a third-country national, for updating their file and for consulting the system in performance of their tasks.\textsuperscript{1360} Stamping will be abolished and an automated calculator will indicate the maximum authorised duration for stay, which will alert to overstayers upon exit.\textsuperscript{1361} However, instead of automated alerts, the revised proposal envisages a mechanism of automatic lists of persons without an exit record that will be at the disposal of the designated national authorities.\textsuperscript{1362} The EES will further assist in scrutinising visa applications\textsuperscript{1363} or for examining applications for access to national facilitation programmes.\textsuperscript{1364}

\textbf{3.2.4 Law enforcement access}

In view of the Council’s desires, consultation of EES data for criminal law purposes will be allowed from the outset of EES operations on the basis of rules that are a mixture of Eurodac and VIS provisions. In particular, as in the case of Eurodac, access will be allowed solely for the purpose of preventing, detecting and investigating terrorist crimes specified in Articles 1 to 4 of Framework Decision 2002/475/JHA on combating

\textsuperscript{1355} ibid art 32(6).
\textsuperscript{1356} ibid art 8(2).
\textsuperscript{1357} ibid arts 8(2) and (3).
\textsuperscript{1358} ibid art 8(1).
\textsuperscript{1359} ibid art 9(1).
\textsuperscript{1360} ibid art 21.
\textsuperscript{1361} ibid art 10.
\textsuperscript{1362} ibid art 11. As noted in the Explanatory Memorandum, for overstayers not yet found at the end of the retention period, a SIS alert could be issued on the basis of a national decision.
\textsuperscript{1363} ibid art 22.
\textsuperscript{1364} ibid art 23.
terrorism, or other serious crimes that are specified in Article 2(2) of EAW Framework Decision, if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

Member States will have to designate law enforcement authorities authorised to consult the EES data, not excluding intelligence agencies. A list of these bodies will have to be communicated to the Commission and eu-LISA, published in the *Official Journal of the EU*, along with any future amendments. As in the case of the VIS, a Central Access Point designated at the national level will verify that the conditions of access are met. That authority will also have to be responsible for the prevention, detection or investigation of terrorist crimes or other serious offences and may form part of the same organisation that made the access request. However, it must act independently when performing its tasks. More than one Central Access Point may be designated to reflect the organisational and administrative structure of the Member States. The operating units will be kept in a list at the national level, but the designated Central Access Points must be communicated to eu-LISA and the Commission and made public. Europol shall also designate an authority that may request access as well as a specialised unit to verify that the conditions of access are met.

Requests for access will be forwarded by the operating units to the central access point which will verify the conditions under rules similar as the ones prescribed in Eurodac and the VIS. Systematic searches are explicitly precluded and the conditions of access bear resemblance to the ones prescribed in the recast Eurodac Regulation. However, the criterion of 'reasonable grounds' is defined as met ‘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 [the] Regulation’. National authorities must have conducted prior searches in national databases without success, and in cases of fingerprints, searches in national AFIS of the Member States

---

1365 See n882-3.
1366 See n596.
1367 Commission, ‘EES proposal of 2016’ (n982) art 3(1)(27).
1368 ibid arts 26(1) and (2).
1369 ibid art 26(3).
1370 ibid.
1371 ibid.
1372 ibid arts 26(4), 26(5).
1373 ibid art 27.
1374 ibid art 28.
1375 See Chapter 4, Section 3.4.2.
1376 Commission, ‘EES proposal of 2016’ (n982) art 29(1)(c).
pursuant to the Prüm Decision.\textsuperscript{1377} Search keys differ depending on the function of the EES as a criminal identification or intelligence tool. In the former case, searches may take place on the basis of biometric data, including latent fingerprints.\textsuperscript{1378} In the latter case, where examination will involve the travel history of a known suspect, perpetrator or suspected victim, search keys are the name, date of birth, nationality or nationalities, and sex, travel document or visa details, biometrics and data on timings of entry or exit and border crossing points.\textsuperscript{1379} Finally, access by Europol is foreseen under the same conditions as the ones prescribed in the Eurodac Regulation.\textsuperscript{1380}

\subsection{3.2.5 Other provisions}

Transfer of data to third countries, international organisations and private parties is allowed by way of derogation solely in order to prove the identity of the third-country national concerned. Such transfer is subject to the same conditions as encompassed in Article 31 of the VIS Regulation.\textsuperscript{1381} As for transfer in the context of law enforcement, this is forbidden altogether, even if that data are further processed at the national level or between Member States.\textsuperscript{1382} Individual rights are redrafted; third-country nationals will have to be provided with the following information: an explanation, using clear and plain language, of the fact the EES will be accessible by law enforcement authorities and Europol; the obligation on visa exempt third-country nationals to be fingerprinted; the obligation on all third-country nationals subject to EES to have their facial image recorded; the mandatory collection of the data for examining entry conditions; the existence of their rights and the procedures to enforce them.\textsuperscript{1383} Their rights of access, deletion and correction are very similar to the ones prescribed in the Eurodac Regulation.\textsuperscript{1384} Supervision is entrusted to national DPA’s and the EDPS in provisions identical to those included in the VIS Regulation.\textsuperscript{1385}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{1377}See n1121. Member States generally did not agree with the exhaustion of searches in other databases. Council, Document 11635/15 (n1331). Prior search does not have to be conducted where 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.
\item \textsuperscript{1378}Commission, ‘EES proposal of 2016’ (n982) art 29(4).
\item \textsuperscript{1379}ibid art 29(5).
\item \textsuperscript{1380}ibid art 30.
\item \textsuperscript{1381}ibid arts 38(1), (2) and (3).
\item \textsuperscript{1382}ibid art 38(4).
\item \textsuperscript{1383}ibid art 44.
\item \textsuperscript{1384}ibid art 45. The rules include the case where visa-related data are factually incorrect or unlawfully recorded.
\item \textsuperscript{1385}ibid arts 49-51.
\end{enumerate}
\end{footnotesize}
4. Evaluation of the EES in light of Article 7 EUCFR

4.1 Application of Article 7 EUCFR

The proposed Regulation aims at establishing a gigantic Schengen-wide database in which biographic, sensitive and travel data collected from most categories of third-country nationals crossing the EU external border will be stored. By now, it is well established that the routine collection and storage of personal data by public authorities falls within the realms of protection under both Articles 8 ECHR and 7 EUCFR, and any subsequent use of the data on the basis of enlarged access, such as law enforcement access, amounts to a separate interference with privacy.\(^\text{1386}\) As observed by the EDPS:

‘Access would fit in the general trend to grant law enforcement authorities access to several large-scale information and identification systems […] and would also constitute a further step in a tendency towards giving law enforcement authorities access to data of individuals who in principle are not suspected of committing any crime’.\(^\text{1387}\)

In comparison to the VIS, which, as argued in Chapter 3, allows for the construction of profiles of visa applicants’ lives,\(^\text{1388}\) the EES is primarily intended to record entry and exit data, and is not oriented at gathering information on the background of each individual traveller, such as their occupation or the motivation behind their visit. However, just like the VIS, the EES will allow authorities to fully monitor the movements of third-country nationals in and out of the Schengen area over a considerable period of time, including the timings and preferred destinations. It may reveal travel habits or preferred routes, as well as the existence of personal or professional relations and ties with residents or organisations in particular States, even if these are not fully traceable. By requiring the collection and storage of data at both entry and exit, travellers will feel that their movement is placed under surveillance, even though in the vast majority of cases this mobility will stem from legitimate, everyday activities, such as leisure or business trips, without intentions of ‘extending their welcome’ to the Schengen territory. It is observed that visa holders will be subjected to an additional layer of surveillance, as on top of the processing of a rather extensive series of data within the VIS, further data will be available in their respect. Key is the

\(^{1386}\) Digital Rights Ireland (n326) ¶35.
\(^{1387}\) EDPS, ‘Opinion of the European Data Protection Supervisor on the proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)’ [2014] OJ C32/25 (executive summary) ¶68.
\(^{1388}\) See Chapter 3, Section 4.1.
fact that the VIS and EES are destined to be interoperable. Therefore, in respect of visa holders, the limitation of their privacy rights is deeper, because competent authorities having access to their data shall be able to construct an even more complete profile regarding their travel history. As for persons against whom a refusal of entry has been recorded, based on the EES, their entry to the Schengen area may be further impaired even if their subsequent visit does not pose any concerns, thus interfering with their right to private life in the form of free movement.\(^{1389}\) Furthermore, as with the previous case studies, the EES interacts with the right of private life through the registration of biometric data. It is recalled that in *S and Marper* the ECtHR found that fingerprints contain unique information ‘capable of affecting the private life of an individual’,\(^{1390}\) an approach embraced by the CJEU in *Schwarz*. Moreover, as noted in Chapter 1, by analogy, taking photos amounts to an interference with the right to private life.\(^{1391}\) Finally, it must be noted that third-country nationals subjected to the forthcoming EES cannot be considered as consenting to the collection and further processing of their personal data. The proposed Regulation will impose compulsory enrollment requirements for entering in and exiting from the Schengen territory. Therefore, almost all third-country nationals who will wish to travel to the Schengen area will be subjected to this procedure.

The limitation to privacy must be considered as wide-ranging, and thus particularly serious, for two main reasons. Firstly, the size of the forthcoming scheme must be taken into account. The EES will constitute by far the largest EU centralised system; a preview of the estimated figures is that in 2015, over 50 million third-country nationals visited the EU, accounting for more than 200 million border crossings.\(^{1392}\) By 2025, 76 million third-country travellers with 302 million border crossings are expected.\(^{1393}\) The storage will enable extensive background checks at points of entry and within national territory. In light of the above, whereas the VIS signified for visa applicants that their choice or need to visit the Schengen area means the abolition of a significant chunk of their privacy, the development of the EES extends this *status quo* to almost all third-country nationals, and indicates that it is an EU prerogative to treat all non-EU nationals with suspicion, as potentially risky, irrespective of any personal circumstances. Such suspicion, which is further evident by allowing police authorities and Europol to access the data, is sufficient for deploying techniques of mass surveillance. Secondly, the fact

\(^{1389}\) See Chapter 1, Section 4.4.
\(^{1390}\) *S and Marper v UK* (n194) ¶84.
\(^{1391}\) See Chapter 1, Section 4.4.
\(^{1392}\) Commission, ‘Stronger and smarter information systems’ (n585) 2.
\(^{1393}\) Commission, ‘Technical Study’ (n706) 22-3.
that the EES will require the collection and further processing of two different types of sensitive data is crucial as it accentuates the feeling of surveillance.\(^\text{1394}\)

### 4.2 Essence of privacy

By analogy to the line of thinking in Chapter 3,\(^\text{1395}\) it could be argued that the case of the EES and the mass collection and further processing of two categories of biometric data (which are sensitive data) goes to the core of privacy protection, particularly since it involves a huge pool of the unsuspected population.

### 4.3 Objective of general interest

The EES purposes broadly involve the improvement of border management, the prevention of irregular migration by assisting in the identification of overstayers, and recording refusals of entry and reinforcing internal security and the fight against terrorism and serious crime, which is considered as an ancillary objective. In Schwarz, the CJEU recognised the fight against identity theft and irregular migration as constituting objectives of general interest,\(^\text{1396}\) whereas in Digital Rights Ireland it found the fight against terrorism and other serious crimes as of utmost importance.\(^\text{1397}\) The management of external borders is a long-standing policy aim of the EU since the abolition of internal border controls. In this context, it must be considered that the EES pursues objectives of general interest of the EU.

### 4.4 Is the limitation ‘provided for by law’?

As analysed in previous chapters, this condition requires that the measure in question is accessible and sufficiently foreseeable, which means that it provides adequate indication as to the circumstances in which, and conditions on which, it allows the authorities to resort to measures affecting their privacy. The original proposal suffered from lack of clarity, particularly with regard to the definition of its

---

\(^{1394}\) See Chapter 3, Section 4.1.  
\(^{1395}\) See Chapter 3, Section 4.2.  
\(^{1396}\) Schwarz (n320) ¶36-8.  
\(^{1397}\) Digital Rights Ireland (n326) ¶41-44.
purposes.\textsuperscript{1398} Admittedly, the Commission has made significant efforts in the revised proposal to fulfill the ‘foreseeability’ requirement by elaborating on the objectives pursued. However, this provision is still unsatisfactory, not only because there seems to be confusion between objectives and functions of the EES, but also because a hierarchy among the ‘shopping list’ of purposes is unclear. The CJEU has consistently held that ‘the choice of the legal basis for an EU measure must rest on objective factors amenable to judicial review, which include the aim and content of that measure’.\textsuperscript{1399} It has explained that when examining a measure, and it is found that it pursues two aims or that it has two components, and if one of those aims or components is identifiable as the main one and the other is merely incidental, the measure must be founded on a single legal basis, in particular the one required by the predominant aim. However, if a measure simultaneously pursues a number of objectives which are inseparably linked without one being incidental to the other, so that various provisions of the TFEU are applicable, such a measure will have to be founded, exceptionally, on the various corresponding legal bases. In the present case, it is unclear whether the enhancement of border controls is the primary aim. A clear provision in this regard is indispensable for assessing the proportionality of the measure, because it is against this purpose that the features of the database will need to be assessed.

\textbf{4.5 Proportionality test}

In Digital Rights Ireland the Grand Chamber found that:

‘[t]he extent of the EU’s legislature may prove to be limited, depending on a number of factors, including, in particular the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference’.\textsuperscript{1400}

In Chapter 3, I noted that the primarily administrative nature of the VIS, coupled with the important role played by the protection of personal data in view of the right to private life, and the extent and seriousness of the interference with that right caused by the setting up of that database, significantly delimit the margin of discretion enjoyed by the EU legislator. Given that the EES is aimed at upgrading border controls and assisting in the fight against irregular migration, thus also framed as an immigration law instrument, the aforementioned conditions are equally applicable in the present case.

\begin{flushleft}
\textsuperscript{1398} EDPS, ‘Opinion on the EES and RTP proposals’ (n1387) 7.
\textsuperscript{1399} Case C-130/10 Parliament v Council (19.07.2012) ¶42-44.
\textsuperscript{1400} Digital Rights Ireland (n326) ¶47. Also see Chapter 1, Section 4.3.3.
\end{flushleft}
4.5.1 Proportionality of the EES as an immigration control tool

Since the release of the original proposal, the necessity of the EES as a tool for improving the management of external borders and preventing irregular migration has been strongly doubted. The optimisation of checks at EU external borders is the flagship of the proposed Regulation, according to which the forthcoming EES will address ‘border checks delays and improve quality of border checks for third-country nationals’. The main motor in this respect would be the abolition of stamping and the replacement of manual checking of stamps with the examination of electronic entries in the database. As the Commission submits, stamps are sometimes difficult to interpret, because they may be ineligible, or the result of counterfeiting. Furthermore, visa authorities processing visa applications experience difficulties to establish the lawfulness of previous visas on the basis of pre-existing stamps. These proclamations are rather misleading. Firstly, the revised proposal seems to disregard the fact that the enrolment of biometric data will add to the border crossing time and will effectively lead to longer waiting times, thus hindering border controls. This issue has been confusing and contentious. Initially, the former EU Commissioner noted that the use of new technologies would enable ‘smoother and speedier border crossing for third country citizens who want to come to the EU’. This premise was based on the abolition of stamping and the establishment of the RTP, a project that is, however, discarded, at least for the time being. In the previous years, the prevailing and rather optimistic perception was that the time necessary for checks would be cut down from 1-2 minutes to below 30 seconds. The pilot and technical studies carried out in between the two proposals found that the added duration of the border-control process is directly linked to the number of fingerprints enrolled and the desired quality. During the pilot, the enrollment of four fingerprints, which is the preferred choice, had the least impact on time by adding 17-20 seconds, and is considered to have a relatively limited impact on the border-crossing process. However, there is no reliable information regarding the enrolment process at land borders, where the implementation of the EES is particularly contested. Furthermore, significant delays will be experienced also upon exit, as the person concerned will have to mandatorily verify their identity through

1401 Commission, ‘EES proposal of 2016’ (n982) 2.
1402 ibid.
1403 Article 29 DPWP, ‘Opinion 05/2013 on Smart Borders’ (WP206, 2013) 5; Meijers Committee, ‘Note on Smart Borders’ (n1330) 2. On the importance attributed to this matter see Council, Document 5815/14 (29.01.2014) 2.
1404 Commission, ”Smart borders”: enhancing mobility and security” (Press release, 28.02.2013).
1405 Commission, ‘Smart Borders’ (n1291.) 12.
1406 eu-LISA, ‘Testing the borders of the future’ (n1301) 5.
fingerprints. It is recalled that since late 2014, verification of fingerprints at external borders is mandatory upon exit for visa holders, but currently there is no information as to whether this has resulted in longer queues.\footnote{1407} Moreover, in numerous States, the travel documents are not machine-readable, therefore the capture of a facial image will add to the border crossing time.\footnote{1408} Another ‘neglected’ factor is the size of the border crossing point. As observed in the 2014 Technical Study, the impact of the EES will be more significant and complex to handle at smaller border crossing points.\footnote{1409} Furthermore, it is unclear how the system will perform in cases where fingerprints cannot be captured on a first attempt, or if the weather conditions are challenging. In light of the above, the modernisation of external checks takes place solely to the benefit of border guards, who will not have to read and interpret previous stamps as part of checking the travel history of a traveller. Assisting border guards to perform checks on travellers comes at the price of a time-consuming process, particularly when entering the Schengen territory for the first time. Besides, the effectiveness of the EES in calculating short stays may be undermined by the possibility of enrolling inaccurate data,\footnote{1410} which has already been recognised as an inevitable collateral effect.\footnote{1411} As such, the effectiveness of the EES is significantly undermined.

Another major driving force for introducing the EES is its expected added value in tackling the problem of overstayers, which is also pursued by the VIS.\footnote{1412} The identification and detection of overstayers on the basis of the forthcoming system will take place on a limited scale only. According to Article 11 of the revised proposal, the system will include a mechanism that will automatically identify which records do not have exit data following the expiration date of the authorised length of stay and the list of presumed overstayers will be at the disposal of national authorities. Although in comparison to the original proposal, the EES will not generate automatic ‘alerts’, the underlying reliance on the effectiveness of the list remains fundamentally flawed. This is because the system will provide no further indication as to the possible whereabouts of each listed individual.\footnote{1413} National competent authorities will still have to locate the listed persons and ascertain their overstay status. In effect, no immediate action will be taken. In an area without internal border controls, the listed person may be present in the

\footnote{1407} See Commission, ‘Sixth bi-annual report on the functioning of the Schengen area 1 May - 31 October 2014’ (Communication) COM(2014) 711 final.\footnote{1408} Commission, ‘Technical Study’ (n706) 79-80. According to the study, if the proposal would be amended so as to include a photo taken live this will add around 40 seconds to the process.\footnote{1409} ibid 106.\footnote{1410} Article 29 DPWP, ‘Opinion 05/2013’ (n1403) 6.\footnote{1411} Council, Document 13193/15 (n1344).\footnote{1412} See Chapter 3, Section 3.2.2.\footnote{1413} Meijers Committee, ‘Note on Smart Borders’ (n1330) 2; EDPS, ‘Opinion on EES and RTP proposals’ (n1387) 8.
territory of another Member State. Furthermore, the lack of proper exit may be attributed to numerous reasons, such as hospitalisation, imprisonment, irregular border crossing, regularisation or death.\textsuperscript{1414} Besides, it is possible that the system itself is malfunctioning or inaccessible.

Moreover, a significant point of concern is the uncertain extent to which the information from the EES will assist in the implementation and execution of return procedures. As the Commission has found, over the past years, there is not only a decrease in the number of apprehensions by around 30\%, but there is also a considerable gap between the persons issued with a return decision and those who, as a consequence, have left the EU.\textsuperscript{1415} This gap is only partly due to the lack of cooperation on behalf of the individual concerned. The lack of cooperation from the non-EU country of origin or transit (e.g. problems in obtaining the necessary documentation from non-EU consular authorities) is also a significant concern, which the EES will not address.\textsuperscript{1416}

Importantly, the insistence on establishing the EES grounded on biometric identification seems to ignore the problematic US model, which, more than 12 years after its establishment is still not in full force. As explained in Section 1, the US agencies have been unable to produce reliable data on overstayers and effectively use the system for tackling this issue. One could counter-argue that the pilot project was meant to mitigate these concerns, however, judging from the delays in implementing the SIS II and the VIS and the complexity of EU external borders, it is difficult to foresee a future EES without the problems of the US-VISIT/OBIM Programs.

As for the fact that the system will allow for an evidence-based approach via the analysis of statistical data, undoubtedly the EES shall generate information on ‘the size and trends of movements across the external borders, especially with regard to irregular migration’.\textsuperscript{1417} Furthermore, it could provide precise data as to whether there is a specific problem with overstayers of certain nationalities. However, the establishment of a computerised system cannot be justified merely to better understand the migration phenomenon and, therefore, rationalise its own existence.\textsuperscript{1418} A policy choice based on a lack of data is unjustified when such data are required to prove the necessity of the proposed instrument.

\textsuperscript{1414} Hayes and Vermeulen (n1290) 41-2.
\textsuperscript{1415} Approximately 484 000 persons in 2012, 491 000 in 2011 and 540 000 in 2010) and those who, as a consequence, have left the EU (approximately 178 000 in 2012, 167 000 in 2011 and 199 000 in 2010. See Commission, ‘EU return policy’ (Communication) COM(2014) 199 final, 3.
\textsuperscript{1416} Meijers Committee, ‘Note on Smart Borders’ (n1330) 2.
\textsuperscript{1417} Commission, ‘Impact Assessment of 2013’ (n1296) 26.
\textsuperscript{1418} Meijers Committee, ‘Note on Smart Borders’ (n1330); Article 29 DPWP, ‘Opinion 05/2013’ (n1403) 3.
Finally, whereas it is true that none of the existing systems addresses the monitoring of third-country nationals who are not subject to visa requirements, it is unfortunate that the EES has been proposed before a thorough evaluation of the VIS is released. It is recalled that the phased roll-out of that system concluded in early 2016, and an evaluation report is due in autumn 2016. Such a report could provide feedback *inter alia* on whether the VIS is an appropriate and effective tool to combat the problem of overstayers.

Bearing in mind that the main aims pursued will only be fulfilled to a limited extent, serious proportionality concerns are raised particularly due to the significantly high number of persons who will be subjected to the modern border crossing procedure; the EES will constitute a huge database, containing massive amounts of personal information on almost all categories of third-country nationals admitted for a short stay, meaning that they will effectively be under surveillance. It will require the collection and further processing of a series of data on a large scale, incomparable to the currently largest information system, the VIS. In effect, almost every third-country national wishing to enter the Schengen territory will have to be enrolled in the system on a mandatory basis. Admittedly, the proposed Regulation excludes certain categories of third-country nationals, either because they have some type of link or relationship with persons enjoying free movement, or due to territorial proximity to the EU. However, as highlighted in Chapter 3, the position of third-country nationals who are family members of EU nationals or persons enjoying the right of free movement, but who do not hold a residence card, are not covered.\(^{1419}\) Another category of nationals that could have been excluded are Turkish nationals falling under the Association Agreement and their family members, in view of the standstill clause in Decision 1/80 and the non-discrimination clause in Article 9 of the Association Agreement.\(^{1420}\) In all other cases, the control will take place in an indiscriminate manner irrespective of whether the person concerned poses a risk of overstay, the legitimate reasons for visiting a Member State, the frequency of their travels, or their age. Fingerprinting will not take place for minors below the age of 12, but registration on the basis of the remaining data will still take place. Millions of third-country nationals will thus be subjected to mass surveillance merely for reasons related to assisting border guards and other competent authorities in carrying out more effective personal assessments of their risk without having the, sometimes, cumbersome task of interpreting stamps. However, stamping and centralised storage cannot be deployed in an interchangeable manner. The current process of stamping has the advantage that the movement of individuals is depicted

\(^{1419}\) See Chapter 3, Section 4.5.1.

\(^{1420}\) Meijers Committee, ‘Note on Smart Borders’ (n1330.) 3.
solely within the passport, which, as the CJEU opined in Schwarz, belongs to the owner.\textsuperscript{1421} Therefore, any competent authority has access to the travel history solely when it is handed over for a specific procedure, such as border control.

Furthermore, proportionality concerns are raised with regard to the registration of biometric data. In addition to the expected congestion at border crossing points, which undermines the facilitation of border controls for third-country nationals, and the negative example of the US-VISIT/OBIM that the EU legislator imitates, a few more points are raised. Arguments regarding over-reliance on biometric data and the possibility of false matches, as detailed in previous chapters,\textsuperscript{1422} are also applicable in relation to the EES. The possibility of a false match in the present case would amount to a possible refusal of entry, as the system enables, and favours, automaticity. The possibility of false matches is multiplied in large-scale information systems where millions of entries are stored, and the EES will constitute the largest database. Admittedly, in comparison to currently operational systems, the proposed Regulation requires the registration of four fingerprints only. This reduction had been proposed already since 2013, when the EDPS observed that 10 fingerprints ‘would only be needed if [the system] pursues a different purpose, i.e. the identification of traces in law enforcement context’.\textsuperscript{1423} However, this change has been accompanied by the addition of a second type of sensitive information, a facial image, as it has allowed for the reduction of fingerprints registered whilst enabling the same result in terms of accuracy of the identification.\textsuperscript{1424} Strikingly, the reason behind the revised rule stems from the need to minimise the additional time for border crossing, rather than from fundamental rights concerns. The recent Technical Study admits that the registration of 10, or even 8 fingerprints, in all types of border crossing points and under various conditions may prove to be a challenging task.\textsuperscript{1425} This is a potentially dangerous line of thinking, as it devalues the impact on privacy through subjecting individuals to mandatory fingerprinting and substitutes the fundamental rights assessment to an exercise of what is technically feasible. In this respect, it is recalled that enrollment on the basis of less than a full set of fingerprints was the policy option implemented in the US, until replaced by a requirement to register all fingerprints. Having this in mind, there is no guarantee that this approach will not be followed at EU level in the future, under the logic of aligning the rules in all operational databases and/or maximising its effectiveness for law enforcement purposes, as advocated when discussing the proposal.
of 2013. Furthermore, this change does not take into consideration the fact that around 47% of people have found that fingerprinting for the purposes of the EES compromises their privacy, whereas one fifth finds this procedure very humiliating. Besides, no NEES processes biometric data and, therefore, such insertion would not correspond to a national practice that is ‘uploaded’ at EU level.

Moreover, in relation to the retention period, the revised proposal marks a departure from the rule previously proposed, which made a distinction between bona fide and mala fide travellers. Under the proposed regime, each entry/exit record or refusal of entry record linked to an individual file will be stored for five years. The same would apply for each individual file. The sole derogation involves third-country nationals who are family members of EU nationals, or other beneficiaries of free movement, and who do not hold a residence card, in which case the data shall be stored for one year. Although in the previous section it was observed that the five-year retention period was advocated in view of allowing police authorities and Europol to consult the EES data and to align with other schemes, particularly the VIS, the ‘official’ reason now is that this ‘one-size-fits-all’ rule will reduce the re-enrolment frequency whilst allowing border guards to perform the necessary risk analysis required by the SBC before authorising a traveller to enter the Schengen area. In the Commission’s own words, ‘[i]t would be a regression of useful information compared to what the border guard currently uses’. This is a valid point, which, however, disregards the different nature of a travel document as opposed to storage in a computerised system, as explained above. Furthermore, there is no universal rule regarding the validity of a passport, with numerous States, such as the US, issuing such documents valid for ten years. It is doubtful that this would justify a further extension of the retention period of data. Therefore, on the basis of S and Marper and Digital Rights Ireland, the retention period must be differentiated as in the withdrawn proposal. A six-month retention period was logical, since according to the SBC ‘it is the minimum period required for the calculations of the duration of the stay’. On the contrary, in the case of overstayers, a five-year retention period could violate a person’s privacy in the form of free movement, as they not be able to re-enter the EU during those five years, even if

1427 Commission, ‘Technical Study’ (n706) 113.
1428 Commission, ‘EES proposal of 2016’ (n982) 5. This argument was submitted in Council, Document 12860/13 (31.07.2013), but the Commission ‘did not consider that storing the travel history […] more than 181 days was justified, bearing in mind that such data could be stored for a maximum of five years in cases of mala fide travellers’.
1429 ibid.
1430 ibid recital 16.
the overstay had taken place for reasons that are not attributable to them.\textsuperscript{1431} The same applies to records on a refusal of entry, as this may pre-empt border guards to refuse entry to the Schengen area on a subsequent attempt solely on the basis of such a record. As for advanced erasure of data, the proposed Regulation is silent as to what happens if the person acquires international protection.\textsuperscript{1432}

In addition, similar concerns as the ones raised in previous chapters regarding the wide range of authorities granted access to the systems without further control or review at EU level apply to the present case as well.\textsuperscript{1433} Finally, with regard to the rights envisaged in the proposal, the right of information could be further amended to ensure that individuals are informed on the purposes for which the EES will be used, apart from the criminal law ones, the categories of recipients of the data and the data retention period. As for transfer of data to third parties, Article 38 of the revised proposal is almost identical to Article 31 of the VIS Regulation; therefore the points raised in Chapter 3 are also relevant in the present case.\textsuperscript{1434} An evaluation of the implementation of this provision prior to the adoption of this rule is necessary in order to identify whether the transfer of data to third parties has led to a violation of the fundamental rights of the persons whose data have been transferred, particularly in cases where there is a risk of non-refoulement.

\textbf{4.5.2 Proportionality of the EES as a law enforcement tool}

Until the withdrawal of the original proposal, opening up EES data to police authorities and Europol was a particularly contested issue and the Commission was not an enthusiastic supporter of this idea. In the Impact Assessment accompanying the Communication of 2008, it took the view that ‘the entry/exit system does not bring any new dimension to the prevention of terrorism’.\textsuperscript{1435} In the proposal of 2013, the Commission contended to subject this additional functionality on the results of an evaluation three years after the database would become functional, cautiously opining, however, that ‘the total negative impact […] could be seen as potentially disproportionate’.\textsuperscript{1436} Currently, it is taken for granted that law enforcement authorities

\textsuperscript{1431} Meijers Committee, ‘Note on Smart Borders’ (n1330) 4.
\textsuperscript{1433} See in particular Chapter 3, Section 4.5.5.
\textsuperscript{1434} ibid. Also see Meijers Committee, ‘Note on Smart Borders’ (n1330) 4; EDPS, ‘Note on the EES and RTP proposals’ (n1387) ¶71-3.
\textsuperscript{1435} Commission, ‘Impact Assessment of 2008’ (n1283) 36.
\textsuperscript{1436} Commission, ‘Impact Assessment of 2013’ (n1296) 39.
will have access to the EES from the outset of its operation, as the ‘evaluation’ of necessity already took place during the negotiating phase.

Apart from the costs of the systems, two more substantial lines of argument have been inferred in this regard; the effectiveness of NEES and the use of the VIS as a law enforcement tool. With regard to the former argument, on the basis of a questionnaire distributed among Member States, the details of five cases only are disclosed, four of which would be inapplicable in the present case. The first case involved a working hypothesis that the offender of a child murder that took place in the border region of a Member State was residing in a neighbouring country. However, no further information as to its actual usefulness was provided and, importantly, since the EES will not record the entries and exits of persons facilitated by the local border traffic, it would be doubtful whether such a consultation would take place in the forthcoming system. Furthermore, it would involve the systematic examination of all entries and exits from the country at a specific time and, therefore, the limited conditions of access may not be fulfilled. In another case of tobacco smuggling, national authorities investigated the travel history of a known tobacco smuggler, only to find that two other persons had been travelling on the same flights as he did. Consequently, the two passengers were caught red-handed at the airport. Such consultation would not require an EES, but an examination of API or the forthcoming EU PNR system would suffice. The third example involves a transnational case of luxury car thefts, where information was used to trace vehicles and couriers, and to document their movements for the purposes of pre-trial investigation and court proceedings. Given that the EES surveys the movement of persons, it is uncertain whether this is a relevant example. The fourth case involved a smuggler who was an EU national known to the authorities and had an accomplice operating in Moscow who, apart from his Afghan nationality, was unidentified. The testimony of an irregular migrant that the accomplice had travelled from one Member State to another was helpful in that the former requested NEES data from the latter. On the basis of that data, including a photo, the witness recognised the accomplice against whom an EAW was issued and the person was arrested. In the case of the EES, however, identification of a person unknown may only take place on the basis of fingerprints or a facial image and not on the basis of travel information.

---

1438 ibid 5.
1439 ibid 6.
1441 See n35.
1442 Council, Document 13680/13 (n1437) 6.
1443 ibid 6.
The sole relevant example involves the conviction of a person for aggravated offences relating to procurement for prostitution and narcotics, where on the basis of NEES data, the professional character and continuity of procurement was proven and the proceeds of the crime were defined. The lack of information, which has been recognised by the Commission, cannot be underestimated. It demonstrates that the added value of law enforcement access to the system is far from proven and, as the Commission claimed in previous years, cannot be quantified. Furthermore, it demonstrates that the timing of the proposal is problematic. Given the sheer amount of data retained in the EES, the number of third-country nationals affected, and the impact on individuals, the need for presenting salient cases becomes all the more pressing.

The second line of argument involves the first findings on law enforcement access to the VIS. The Technical Study of late 2014 found that until 31 March 2014, an average of 11 searches per day were carried out in all participating States. Out of the 11 searches, there were five retrievals per day. Searches and authentications by fingerprints remained very limited throughout that period; only five searches by fingerprints were carried out and there was only one authentication by fingerprints. These data indicate that law enforcement access to the VIS has taken place on a limited basis, probably because at the time when the data were collected the database did not operate at full capacity, or because not all Member States may have implemented the necessary organisational and technical features to access the central VIS. Even so, the more recent data, as presented in Chapter 3, confirm the finding that law enforcement access has been limited. As observed, this finding questions the necessity of law enforcement access altogether.

In light of the above, it is evident that the necessity of law enforcement access is far from proven. In theory, the EES could provide travel histories of third-country nationals who are suspected of terrorism or another serious criminal offence. However, as Peers rightly points out:

‘if a person who entered the Schengen territory subsequently was suspected of involvement in a terrorist offence, the entry-exit system would provide the limited facility of providing information as to whether (and if so, when and where) the suspect had exited that territory legally’. With regard to the proportionality of law enforcement access, the risk of stigmatisation as highlighted in Chapter 3 and 4 is evident also in the present case,
which is enhanced due to the enlarged retention period for ordinary travellers.\textsuperscript{1449} It must be noted that Digital Rights Ireland was released amidst discussions taking place within the Council. However, given that the proposed rules are heavily influenced by the legal framework of the VIS and Eurodac, which have already been analysed and found disproportionate, the proportionality of law enforcement access is equally disproportionate on numerous grounds. In particular, in relation to designated authorities, further criteria could have been introduced as to what type of bodies may be designated for the purpose of access. Regrettably, intelligence services are not excluded. Furthermore, with regard to the conditions of access, a prior review by a court, or at least an independent authority, should take place; verification by the Central Access Point is insufficient.\textsuperscript{1450} Notably, the threshold required in order to grant access was understood ‘in terms of factual basis for showing suspicion of committing a crime’,\textsuperscript{1451} which reminds the ‘factual indications’ proposed in relation to the VIS.\textsuperscript{1452} Nevertheless, this approach was not followed. In addition, the threshold for criminal offences falling within the remits of the EES Regulation is rather low and the possibility of comparing latent fingerprints may lead to increased false matches.\textsuperscript{1453}

A welcomed rule is the fact that transfers are excluded. According to the Commission:

‘[a]ccess for certain third countries for law enforcement purposes would have significant negative implications for data protection having regard to the potentially vast amounts of data that could be shared and the risk of "data mining". It would require the negotiation and conclusion of an extensive agreement with selected third countries to ensure, to the greatest possible extent, that the EU can regulate how and for what purpose such data would be used, and how long it would be stored. Certain third countries may also misuse access to data on their citizens (e.g. political dissidents) for exercising repercussions on the members of their families still present in that third country, which requires a serious analysis into which countries could potentially gain such access and under what strict conditions.’\textsuperscript{1454}

This line of reasoning should also have been preferred in the cases of the VIS and Eurodac.

\textsuperscript{1449} See Chapter 3, Section 4.6; Chapter 4, Section 4.2.
\textsuperscript{1450} Digital Rights Ireland (n326) ¶62.
\textsuperscript{1451} Council, Document 10732/15 (n1331) 6.
\textsuperscript{1452} See Chapter 3, Section 4.6.
\textsuperscript{1453} See Chapter 4, Section 4.2.3.
\textsuperscript{1454} Commission, ‘Impact Assessment of 2013’ (n1296) 29.
5. Conclusion

The forthcoming introduction of the EES will bring Member States one step closer to achieving total control over all cross-border movements of third-country nationals. Modelled on the US-VISIT/OBIM Programs despite their serious shortcomings, the EES will be designed to store en masse biographic, biometric and travel information on many millions of non-EU nationals entering and leaving the Schengen area. This collection of extraordinary amounts of everyday data is framed as ‘filling the gap’, stemming from the lack of information on visa exempt travellers. Apart from constituting a necessary accompaniment of the VIS, the EES is meant to bridge the alleged gap that has been triggered by the growing tendency to rely on political and external relations grounds to justify the removal of countries from the EU visa ‘black list’. In this framework, the EES constitutes a compensatory measure of the EU’s visa policy and marks the continuation and intensification of the preventive logic of surveillance as exemplified by the VIS and Eurodac.

Nevertheless, the necessity of establishing the EES has not been proven; there are reasons to believe that traveller flows will be disrupted due to the mandatory fingerprinting process, and the possibility to detect and return overstayers can only be met to a limited extent. Against this background, proportionality concerns are raised by the fact that the system will encroach upon the privacy of millions of travellers who are, in principle, unsuspected of any misconduct simply in order to ease the work of border guards and identify overstayers who may not be returned to their country of origin. In this respect, stamping and centralised storage cannot be deemed as equivalent policy options. The collection of biometrics, despite the (so far) failed US experiment and the fact there is no comparable biometric NEES, has been flagged by the Council as a necessary parameter of the system. Although the revised proposal takes note of the technical difficulties in capturing a full set of fingerprints, it requires the storage of two types of sensitive data – four fingerprints and a facial image. In this context, surveillance of movement is deepened and collection is restricted, but processing in general is not. With regard to the retention period, the amended rules are disproportionate in that they disregard the difference between the vast majority of travellers who pursue legitimate activities and, therefore, are ‘legal’, and overstayers, whose number is uncertain. As for law enforcement access, it has been demonstrated that, albeit an ancillary aim, it may have significant repercussions on other modalities of the system. In the present case, the Member States’ desire to open up the EES to crime

control agencies has been translated into the compulsory fingerprinting from the outset of the EES operations, and formed part of the discourse on extending the data retention period. Nevertheless, the need for law enforcement access to EES data is disproportionate not only because it unreasonably surrounds almost all non-EU travellers with a cloak of suspicion of criminality, but also because no substantial arguments have been inferred. Furthermore, the release of Digital Rights Ireland did not lead in revisiting the proposed rules, which are a combination of VIS and Eurodac provisions. As such, a series of privacy concerns, as highlighted in Chapters 3 and 4, are raised.

Overall, the setting up of the EES signals an era of disproportionate, generalised and maximised surveillance that is becoming the norm, despite the significant privacy concerns. There is no doubt that in light of the highly securitised legal landscape triggered by phenomena such as that of ‘foreign fighters’, the revised proposal will secure consensus among co-legislators in a fast-track procedure underpinned by an emergency logic. However, the rebranded Eurodac, and the forthcoming EES, are not the sole proposals featuring on the EU agenda regarding immigration databases. For the sake of a holistic approach, the last Chapter briefly maps more ideas that will pre-occupy the EU legislator in the coming years; the RTP (the temporarily abandoned ‘sibling’ of the EES), the ETIAS, the Residence Permits Repository and interoperability among information systems.
CHAPTER 6. ‘The Shape of Things to Come’: EU Immigration Databases in Transition

‘If the EU uses its law enforcement and border control tools to the full, exploits the potential of inter-operability between information sources to identify any security concerns from a common pool of information, and uses the stage of entry into the EU as a key point for security checks to take place, the result will negate the ability of terrorist networks to exploit gaps. This is at the heart of the Security Union.’

1. Introduction

Over the past decade the interest in harvesting the potential offered by technological evolutions has boomed. Following the EES logic of ‘filling gaps’ in information exchange, the EU immigration databases discussed in the previous Chapters are supplemented by a series of suggestions. Some of these ideas have led, or will soon lead, to a Commission proposal, whilst others are still at an embryonic stage. For the purposes of giving insight into the speed and intensity of developments in this field, this last Chapter completes setting the scene of EU immigration databases by concisely outlining these suggestions.

To that end, I discuss in turn the RTP, which was the second component of the original ‘Smart Borders’ package aimed at facilitating the border crossing process for pre-screened and pre-vetted frequent travellers; the ETIAS, according to which visa exempt travellers will have to obtain authorisation prior to their intended journey by supplying a series of information; the possibility of introducing a Residence Permits Repository; and interoperability of databases.

---

1457 Commission, ‘Stronger and smarter information systems’ (n85).
2. The Registered Traveller Programme (RTP): The ‘good’, the ‘bad’ and the ‘ugly’ travellers

2.1 Background information

The idea of speeding up border crossings of pre-approved travellers who are proven trustworthy is not an EU novelty. Similar projects, commonly known as ‘Trusted Traveller Programmes’, are rolling out worldwide, particularly in the US, since the early 2000s, albeit in a limited manner. With reference to the NEXUS, a programme that expedites travel in the US-Canada border, Sparke eloquently captures the two competing forces behind the deployment of these schemes; ‘the economic forces that continue to generate pressure for liberalized cross-border business movement’ as opposed to ‘the political and cultural forces that are leading to heightened border surveillance’. In this context, ‘Trusted Traveller Programmes’ are seen as a digital bridge that can combine both rationales; facilitate economic development whilst ensuring security. One of their key characteristics is the emphasis on speeding up the border crossing of the nationals of the States deploying them. As such, they contribute to the contemporary redesign of citizenship and a configuration of the relationship between the citizen and the State ‘where the experience of one’s national border and the documentation required for one to “fully function” as a citizen is not at the sole discretion of one’s home state’.

Their benefit essentially lies in that pre-clearance enables individualised risk assessment \textit{a priori} on the basis of concrete information without pressure, facilitating pre-emption and identification of risky and dangerous individuals before they reach the actual border. In effect, these schemes constitute a form of ‘social sorting’, as they segregate the travelling population into groups of different security risk; those who have been pre-registered as ‘trusted’ and those who have not been registered and, therefore, have not been designated as trustworthy. In this framework, they allow expedited

\footnote{1458 These are: Global Entry, NEXUS, CENTRI and FAST.} 
\footnote{1459 In the EU, such systems operate in France, Netherlands, UK and Germany. For an overview see FRONTEX, ‘Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports’ (2007).} 
\footnote{1460 Matthew Sparke, ‘Fast Capitalism/Slow Terror – Cushy Cosmopolitanism and Its Extraordinary Other’ in Louise Amoore and Marieke de Goede (eds), \textit{Risk and the War on Terror} (n1201) 133-4.} 
security screening of unsuspected travellers who have been pre-vetted, and a more efficient rearrangement of human and technical resources. In that sense, surveillance is confused for freedom,\textsuperscript{1463} whilst privacy becomes a commodity tradable in exchange for convenience and speed.

2.2 Overview of the proposal

At EU level, similar concerns were raised that an intensification of immigration control would enhance the risk of obstructing ‘wanted flows’, such as foreign businessmen.\textsuperscript{1464} The possibility to circumvent extensive checks for ‘trusted persons’ was first referred to in 2005 and was driven by aspirations for the facilitation of movement in the framework of the EU-US partnership on trade.\textsuperscript{1465} A few months later, the Commission included the establishment of the RTP among its long-term objectives, stating that ‘in order to reduce the checks, a programme could be introduced for known bona fide travellers (i.e. commuters) to facilitate and automate the border-crossing process.’\textsuperscript{1466} In its 2008 Communication on the next steps in border management, the Commission called for the establishment of the RTP next to the EES, explaining that ‘low risk’ third-country nationals could be enabled to acquire the ‘Registered Traveller’ status that could allow them to bypass thorough checks at the borders.\textsuperscript{1467} The 2011 Communication on smart borders identified two principles underpinning its operation: accurate risk management, according to which pre-approval would need to be sufficiently thorough to compensate for alleviating the border check process; and cost-effectiveness, which would mandate wide eligibility criteria that would simultaneously ensure a high level of security.\textsuperscript{1468} Despite concerns about the administrative burden and the limited scope of the RTP,\textsuperscript{1469} the Commission released its proposal as part of the ‘Smart Borders’ package.

\textsuperscript{1463} Didier Bigo, ‘Freedom and Speed in Enlarged Borderzones’ in Vicki Squire (ed), \textit{The Contested Politics of Mobility} (Routledge 2011).
\textsuperscript{1464} Gammeltoft-Hansen (n4) 3.
\textsuperscript{1465} Commission, ‘A stronger EU-US partnership and a more open market for the 21\textsuperscript{st} Century’ (Communication) COM(2005) 96 final, 9 (emphasis added).
\textsuperscript{1466} Commission, ‘Improved effectiveness’ (n780) 9.
\textsuperscript{1467} Commission, ‘Preparing the next steps’ (n1282) 5.
\textsuperscript{1468} Commission, ‘Smart borders’ (n1291)11.
\textsuperscript{1469} Commission, ‘Staff Working Document – Impact Assessment accompanying document to the proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme’ SWD(2013) 50 final, 7. For discussions before the adoption of the proposal see Council Documents 17706/11 (n1295) and 7266/12 (07.03.2012).
According to the Commission, the RTP would offer third-country nationals over the age of 12\footnote{ibid art 5(6)(a).} that travel frequently or regularly to the Schengen area\footnote{ibid art 5.} the possibility to circumvent the ordinary border control process at the external borders by applying for ‘Registered Traveller’ status on a voluntary basis. Holders of multiple-entry visas or residence permits and family members of EU citizens would, in principle, be granted such status.\footnote{Commission, ‘RTP Proposal’ (n1243) art 14(2).} The enrollment would require the collection of a wide range of alphanumeric data,\footnote{ibid arts 25-30.} similar to those prescribed in the VIS Regulation,\footnote{See Chapter 3, Section 3.2.2.} and four fingerprints,\footnote{A number of Member States suggested the introduction of a facial image, whereas others favoured the registration of a full set of fingerprints. See Council, Document 10355/13 (24.06.2013). For a view on verifying through photographs only see Council, Document 8620/15 (07.05.2015).} which would be stored in a centralised database (the Central Depository)\footnote{Commission, ‘RTP Proposal’ (n1243) art 21.} for five years.\footnote{ibid art 34.} A series of supporting documentation\footnote{ibid art 9 and Annex II, which set out an elaborate, but non-exhaustive, list of supporting documents. For reservations regarding this list, including the suggestion for differentiated criteria depending on the different categories of RTP applicants see Council Documents 10355/13 (n1475) and 12753/13 (30.07.2013).} and a personal interview\footnote{ibid art 34.} would also be necessary. On the basis of the collected information, applicants would go through rigorous background checks for pre-screening purposes on the basis of criteria which are aligned to those required for issuing multiple-entry visas.\footnote{Commission, ‘RTP Proposal’ (n1243) art 12.} Successful registration in the system would subtract layers of security checks to the users, since these checks would have taken place at a prior stage – that of pre-approving the application. ‘Registered Travellers’ would be issued a token, which, combined with the travel document and a fingerprint comparison, would suffice for verifying their identity.\footnote{ibid art 12.} National visa and border control authorities would access the data\footnote{ibid art 4.} for performing border checks, examining RTP applications and gathering statistics.\footnote{ibid arts 31-3.} Notably, few Member States expressed their desire to open up this system to law enforcement authorities, with the Commission replying that such access ‘would
not have any added value in the context of the RTP, all the more because of the low-risk travellers who fall under its scope.\textsuperscript{1484} Transfer to third parties would be prohibited under any circumstances.\textsuperscript{1485} During the negotiations a number of issues arose, mainly related to the organisational aspects of the application procedure. A large majority of Member States questioned the necessity of the RTP, claiming that it would entail severe financial and administrative implications for consular posts and border crossing points.\textsuperscript{1486} In order to insert a degree of flexibility, it was suggested that Member States would be able to select the border crossing points and consulates where applications would be collected and processed.\textsuperscript{1487} According to another proposal, Member States could be granted discretion in choosing which national body would collect and process applications for registration in the RTP, including whether applications would be dealt with by institutions, external contractors or representation.\textsuperscript{1488} Other suggestions included the possibility to deviate from the RTP rules, where ‘the applicant and the concerned authority may […] choose the best possible solution based on the interest of both’,\textsuperscript{1489} and the prescription of an online application, whereby personal appearance would merely be of a validating nature.\textsuperscript{1490} The Technical Study on Smart Borders presented an alternative model, according to which prior registration to the EES would be a prerequisite,\textsuperscript{1491} leading to thoughts on building both the EES and the RTP as a single architectural system.\textsuperscript{1492} The necessity of a token was also disputed,\textsuperscript{1493} with the Technical Study concluding that a separate token would add operational complexity, whereas using travel documents for verification would be more effective.\textsuperscript{1494} Although the RTP proposal was withdrawn, the added value of the RTP approach is largely recognised. Prior to the adoption of a revised ‘Smart Borders’ package, the Commission noted that in view of facilitating and accelerating border crossing ‘for the largest

\begin{footnotes}
\footnote{1484} Council, Document 10355/13 (n1475) 2.
\footnote{1485} Commission, ‘RTP Proposal’ (n1243) art 42.
\footnote{1486} See Council, Documents 10355/13 (n1475); 14198/13 (04.10.2013); 17487/13 (10.12.2013); 17981/13 (20.12.2013). The Commission had already expressed its view that if participation to the RTP would be on a voluntary basis, ‘it would be difficult to ensure a fair and balanced distribution of administrative burden’. Also see Council, Document 6802/14 (19.03.2014).
\footnote{1487} Council, Document 10355/13 (n1475) 8.
\footnote{1488} Council, Document 13806/13 (n1326).
\footnote{1489} Council, Document 6802/14 (n1486) 5.
\footnote{1490} Council, Documents 10355/13 (n1475) 8. Also see Council, Document 8620/15 (n1475).
\footnote{1491} Commission, ‘Technical Study’ (n706) 119-22.
\footnote{1492} Council, Document 8964/15 (22.05.2015) 3. The Commission further suggested the so-called ‘Fast-Lane for all’ for busiest crossing points without replacing the RTP. See Council, Documents 11631/15 (08.10.2015); 13270/15 (22.10.2015).
\footnote{1493} Council, Document 13806/13 (n1326) 8.
\footnote{1494} Commission, ‘Technical Study’ (n706) 71-3.
\end{footnotes}
possible category of travellers’ a forthcoming legislative proposal could propose further variations and/or a combination of options.\footnote{1495}

The destiny of the RTP is unknown. Instead of an amended proposal, the Commission has endorsed a flexible approach by putting forward amendments to the SBC concerning the operation of national RTPs.\footnote{1496} Member States are left with the discretion not only to establish a voluntary programme, but also to conclude agreements ensuring that the beneficiaries of their national programmes may benefit from the facilitations recognised by other national programme(s). In this framework, travellers will not undergo extensive checks at EU external borders, if the following conditions are met:

a) A pre-vetting procedure exists and is carried out by visa or border authorities;

b) The applicant fulfils the entry conditions of the SBC;

c) Valid travel document, visa or residence permit, proof of the need or justification to travel frequently or regularly;

d) Proof of integrity and reliability (lawfulness of previous visas, applicant's economic situation in the country of origin, or genuine intention to leave the territory of the Member States);\footnote{1497}

e) Justification of the purpose and conditions of the intended stays;

f) Sufficient means of subsistence;

g) There is no alert in SIS and the applicant is not considered as a threat to public policy, internal security, public health or the international relations of any of the Member States;

h) Access for a maximum of one year, after which a re-assessment must take place;

i) The identity of the third-country national, and the fact that they have valid access to the programme, is verified, and;

k) Access to the programme is revoked if the person no longer meets, or never met, the conditions for granting access.

This is not the end of story. Following the evaluation of the implementation of these rules in three years, the Parliament or the Council may invite the Commission to propose the establishment of an EU programme for frequent and pre-vetted third country national travellers.

\footnote{1495}{Council, Document 14026/15 (17.11.2015).}
\footnote{1496}{Commission, ‘Proposal as regards the use of the Entry/Exit System’ (n1247) art 8e(4).}
\footnote{1497}{For criticism on the flexibility of this criterion see Meijers Committee, ‘Note on Smart Borders’ (n1330) 6.}
2.3 Evaluation of the RTP in light of Article 7 EUCFR

In comparison to the previous cases, the RTP differs in three main respects. Firstly, its underlying rationale is infused by two competing aims; as such, it is not a wholly repressive instrument, but it is driven by the logic of openness and convenience. The function of such schemes is further based on an untested belief that this logic of acceleration in peoples’ lives should trump its implications for fundamental rights. In comparison to the previous cases, the RTP differs in three main respects. Firstly, its underlying rationale is infused by two competing aims; as such, it is not a wholly repressive instrument, but it is driven by the logic of openness and convenience. The function of such schemes is further based on an untested belief that this logic of acceleration in peoples’ lives should trump its implications for fundamental rights. Secondly, it does not target a specific group of third-country nationals, but rather links the acquisition of ‘Registered Traveller’ status to the need to be regularly present in the EU and the subjective criterion of not being deemed risky. Importantly, rather than imposing direct obligations, it is based on the voluntary participation of those travellers who are willing to subject themselves to individualised risk assessments for the sake of their own convenience. At the same time, the RTP is a logical continuation of the developments examined in previous Chapters. Building on the EES logic, which extends the cloak of suspicion over almost all third-country nationals in an indiscriminate manner, the RTP confirms that all third-country nationals are presumed to pose a risk to EU internal security with minimal exceptions. As the EDPS has eloquently pointed out, the starting point:

‘will no longer be that third-country nationals in general are to be considered as entering the Union in good faith, unless specific evidence causes suspicion, but that it would be up to travellers to exculpate themselves by supplying additional information about themselves even in the absence of any evidence’. 1499

Therefore, only those travellers who are willing to take extra steps by subjecting themselves to extensive background checks could revoke this suspicion; an option that would be reserved solely for frequent travellers. In turn, the majority of other third-country nationals who wish to travel to the Schengen zone and are travelling either for the first time or are infrequent travellers, or those who for any reason do not wish to participate in the scheme, would constitute a class of ‘mala fide’ travellers by default.1500 Thus, the idea of the system marks a de facto dichotomy between potentially

1499 EDPS, ‘Opinion on migration’ (n1292) ¶35.
1500 In its early references, the division was more nuanced due to the explicit reference to ‘bona fide travellers’. See Commission, ‘Preparing the next steps’ (n1282). Although in the Commission Communication on Smart Borders, this reference was dropped the bona fide rhetoric is transplanted in the EES. See for instance Commission, ‘EES proposal of 2016’ (n982) explanatory memorandum, 5. For an eloquent criticism on this term see EDPS, ‘Preliminary comments on: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, ‘Preparing the next steps in border management in the European
trustworthy frequent travellers and those who are in principle not trustworthy. The operation of the system would essentially further sort out third-country nationals into ‘good’ travellers (who would be given the ‘green light’ to go through faster border crossings), ‘bad’ travellers (either because they are outside of the scope or not willing to undergo extensive pre-checks), and ‘ugly’ travellers (whose application would be refused, but their data would still be stored in the system).

The creation of ‘kinetic elites’\textsuperscript{1501} through the establishment of another database constitutes a system of surveillance of movement, which is, however, performed in a different manner. As it has been eloquently argued, whereas in Foucault’s ‘panopticon’ the lives of those at the bottom layers of society are fully exposed whilst the upper layers are afforded relative anonymity,\textsuperscript{1502} the RTP runs counter to this paradigm and is closer to the views of Haggerty and Ericson\textsuperscript{1503} that hierarchy of visibility has been leveled, producing non-hierarchical surveillance structures.\textsuperscript{1504} In order to carry out this type of surveillance, the privacy of applicants would be interfered with via the collection and further processing of a wide range of personal data; in addition to basic biographic information and sensitive data, the Central Depository would store information on persons or companies who are liable to pay the applicant’s subsistence costs during the stay, the main purposes of the stay, the applicant’s home address and telephone number and their occupation. In effect, on the basis of RTP information, it would be possible to compile a complete profile about an applicant’s personal and professional life, including any personal or professional ties in the EU, or habits. In fact, by requiring the storage of information on the address and telephone number, the RTP proposal would go even further than the VIS Regulation.

Consent of the applicant is presented as the ground for legitimising the collection and further processing of personal data. Article 7 of the Data Protection Directive lists consent as the first ground legitimising data processing, and is defined

\textsuperscript{1502}Foucault (n25).
\textsuperscript{1503}Haggerty and Ericson (n825) 605.
as ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’. As mentioned in Chapter 1, the General Data Protection Regulation strengthens the concept of consent by requiring it to be ‘unambiguous’ as well. Besides, in cases involving the processing of sensitive data, the threshold is higher by also requiring it to be explicit. As it has been pointed out, the validity of consent depends on whether the person concerned is able to exercise ‘a real choice’, without the risk of coercion or significant negative consequences in case they do not provide their consent. Consent is not freely given if the consequences of consenting undermine the freedom of choice enjoyed by individuals. In the present case, the extent to which consent is freely given is questionable. With the intensification of immigration control through the introduction of additional layers of security checks that are enabled by new technologies, border crossing is morphed into an inconvenient, burdensome and time-consuming process. The introduction of the EES will place further burdens on third-country nationals, possibly causing delays that would make the RTP a favoured option. Given that travellers generally have little leverage in negotiating privacy boundaries, to a certain extent they may be ‘softly forced’ to apply for participation in the scheme, which in effect undermines the validity of their consent.

Overall, the fact that a wealth of personal data would be centrally stored raises serious concerns. Among the proposed models (use of token; combined use of token and centralised storage; centralised storage only), the first one would be the most ‘privacy friendly’. On the basis of Schwarz, a token could store both alphanumeric and biometric data, and verification could still take place on the basis of a travel document and visa if applicable. Centralised storage, with its inherent risks of abuse or possible re-use of data for other purposes, would be averted and the token would remain within the ownership of the RTP user. According to the Commission, a purely token-based system would allow ‘Registered Traveller shopping’, as no data would be stored from previous applications when national authorities assess an application. However, as observed in Chapter 3, centralised storage and storage in a medium should not be

1506 See Chapter 1, Section 3.1.
1509 EDPS, ‘Opinion on the EES and RTP proposals’ (n1387) 18.
1511 See Chapter 1, Section 5.2.1.
1512 Commission, ‘Impact Assessment accompanying the RTP proposal’ (n1469) 35.
considered as comparable and interchangeable options. In order to safeguard applicants’
privacy, national authorities examining a future application could be ‘inconvenienced’
by retrieving further information through direct contact with the issuing authority.

3. European Travel Information and Authorisation System (ETIAS): A flanking measure of the EU’s visa policy

In Chapter 5, I referred to a seemingly forgotten EU project regarding the
establishment of a system processing applications for travel authorisations from all visa-
exempt travellers.\textsuperscript{1513} This idea originally emerged alongside the EES and RTP,
mirroring the US ESTA, but in 2011 the Commission decided not to proceed further
with the preparations,

‘as the potential contribution to enhancing the security of the Member States
would neither justify the collection of personal data at such a scale nor the
financial cost and the impact on international relations’.\textsuperscript{1514}

When the ‘Smart Borders’ proposals were put forward, there were suggestions to
consider including an EU ESTA,\textsuperscript{1515} but there was no follow-up in this respect. The idea
to step up efforts to prevent the entry of potentially risky travellers was, nonetheless, not
abandoned. The growing trend of liberalising visas in several neighbouring countries
has recently led to the multiplication of calls to further strengthen control over visa
exempt travellers.\textsuperscript{1516} The EU Travel Information and Authorisation System (ETIAS), as
it is now called, is viewed as a flanking measure of the EU visa policy, just like the
EES, and as covering the information gap stemming from the lack of background
material on visa exempt nationals. At the same time, the growing interest in ETIAS
should also be seen in the broader context of the highly securitised political framework
in the aftermath of the terrorist attacks in Paris and Brussels. Therefore, in order to
allow law enforcement authorities to have access to data ‘comparable’ to those available
for visa holders,\textsuperscript{1517} visitors will have to register beforehand the relevant biographic
information regarding their intended journey, such as identity and contact details,

\textsuperscript{1513} See Chapter 5, Section 2.2
\textsuperscript{1514} Commission, ‘Smart borders’ (n1291) 7.
\textsuperscript{1515} Council, Document 8018/13 (27.03.2013).
\textsuperscript{1516} Commission, ‘Stronger and smarter information systems’ (n585) 13.
\textsuperscript{1517} ibid.
purpose of the journey and itinerary via the internet.\textsuperscript{1518} Judging from the US approach, such information will resemble the categories of data collected when applying for a visa except for biometrics and the application could be submitted even a few days before the planned visit and the checks would take place almost instantaneously. As for its purposes, in the Roadmap for information exchange that was agreed upon in June 2016, the establishment of such system is viewed as a means of a) collecting applications for authorisation to travel; b) determining the eligibility of foreign nationals to travel for short stays; c) determining whether such travel poses any law enforcement or security risk; and d) preventing a third-country national from travelling whilst retaining the possibility to deny a traveller entry even if travel authorisation has been granted.\textsuperscript{1519} Unsurprisingly, it has already been suggested within the Council that law enforcement agencies could use ETIAS data to combat terrorism and serious crime.\textsuperscript{1520}

The setting up of the ETIAS along these lines currently scores high in the EU agenda. The Commission is conducting a study, due in October 2016, assessing the feasibility and proportionality of such a system. However, the decision seems to have already been taken and a proposal is expected in November 2016. The creation of an ETIAS is a bold move towards preemptive surveillance of movement through extensive risk assessments on the basis of providing a wide range of personal information. As noted by the Dutch Presidency:

'\textit{The possible added value […] lies in the information which is given by the traveller when registering before travelling, in the possibility to assess this information and use it for pre-screening, in a possible deterrent effect on \textit{mala fide} travellers and in the facilitation of the border procedures after a traveller has obtained the travel authorisation.}'\textsuperscript{1521}

The proportionality concerns of such a system are evident. Its establishment will impose an additional layer of control under the assumption that, in principle, all travellers are suspected lawbreakers. The ETIAS will constitute as large a database as the EES and containing as much wealth of personal information as the VIS, thus combining the worst of both worlds, and will be used for a variety of purposes. It will allow authorities to construct complete profiles of visa-exempt travellers who are previously unsuspected of any offence. Coupled with the EES, the ETIAS will constitute both a massive catalogue of third-country nationals and a powerful surveillance tool geared by the logic of risk prevention transplanted once again into immigration control.

\textsuperscript{1518} ibid.
\textsuperscript{1519} Council, Document 9368/1/16 (06.06.2016) 50.
\textsuperscript{1520} Council, Document 8590/16 (03.05.2016).
\textsuperscript{1521} ibid 3. Emphasis original.
4. Holders of residence permits, residence cards and long-stay visas: Next in line?

As noted in Chapter 5, the forthcoming EES exempts from its personal scope holders of residence permits, residence cards and long-stay visas, whose documents are issued under the competence of the Member States.\footnote{1522} Early in the discussions on the original proposal, the issue of whether residence permit holders should be excluded or not was highly contested, with numerous Member States calling for expanding the scope of the database to cover them as well.\footnote{1523} Such an addition would alleviate the Member States concerns and tackle social benefits fraud,\footnote{1524} as in the absence of stamping, such information would be difficult to obtain.\footnote{1525} Certain Member States were also in favour of including holders of residence cards under Directive 2004/38.\footnote{1526} Calls to expand the scope of the EES proliferated, leading the Commission Legal Service to express its doubts as to whether Article 77 TFEU, which provides the legal basis of the EES, could cover such a category, since the main objective of the EES is to facilitate external border control.\footnote{1527} Although the issue will not be further pursued within the auspices of the EES, it will be further examined separately in the following months, thus forming a sort of flanking measure to the abolition of stamping. As for long-stay visa holders, in its Communication on stronger and smarter information systems, the Commission identified the lack of information on long-stay visa holders as a gap.\footnote{1528} It remains to be seen how this issue will be addressed in the future. Even though most Member States do not centrally record such data,\footnote{1529} the Roadmap for information exchange and information management flags up the establishment of a Residents Permits Repository as a way forward, and would store information on residence cards, residence permits and long-stay visas.\footnote{1530} Such a system would fill the last gap in information exchange in terms of scope ratione personae as all third-country nationals will be monitored without exceptions. The underlying logic is the decentralised management of the documents issued, though this has a collateral effect on immigration control. Of particular risk is the fact that the identities of residence card and long-stay

---

\footnote{1522}{See Chapter 5, Section 3.2.2}
\footnote{1523}{Council, Document 9863/13 (n1321) 2, 4.}
\footnote{1524}{Council, Document 7592/15 (01.04.2015).}
\footnote{1525}{For the discussion on the merits of registering residence permit holders see Council, Documents 12527/15 (08.10.2015). See also Council, Documents 9778/15 (22.06.2015); 10469/15 (22.07.2015), 11627/15 (08.09.2015).}
\footnote{1526}{ibid. Citizens Rights Directive (n611) arts 9-11.}
\footnote{1527}{Council, Document 13193/15 (n1344).}
\footnote{1528}{Commission, ‘Stronger and smarter information systems’ (n585) 3.}
\footnote{1529}{Council, Document 12527/15 (n1525).}
\footnote{1530}{Council, Document 9368/1/16 (n1519) 55.}
visa holders cannot be biometrically verified, an issue that is considered ‘a security risk that should be addressed’. Additionally, such a system would be useful in facilitating their border crossing. A study should be conducted to determine whether such a system could be established.

5. Interoperability

The final development that I wish to briefly touch upon is the possibility of interconnecting different databases which has been an important and recurring issue. Debates first started in the aftermath of 9/11, with a key issue being whether the then negotiated VIS could be linked or incorporated into the SIS. After the Madrid bombings, the European Council, in its Declaration on combating terrorism, invited the Commission to submit proposals for enhanced interoperability between SIS II, VIS and Eurodac. In its Communication on improved effectiveness, enhanced interoperability and synergies among EU databases, the Commission defined interoperability as the ‘ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge’. However, details on the legal aspect for the interoperability of databases were spared, as the concept was reduced to a technical rather than a legal or political matter.

For years, interoperability was discussed, albeit in a sporadic manner, without being accompanied by concrete proposals. Since the Paris attacks of 13 November 2015, the connection of the ‘data pots’ has gained fresh impetus. The European Council Conclusions of 18 December 2015 clearly refer to the need to ensure interoperability of all relevant systems to ensure security checks. After the Brussels events of 24 March 2016, JHA Ministers adopted a Joint Statement at their extraordinary meeting in which

---

1531 ibid.
1532 ibid.
1534 Commission, ‘Development of the Schengen Information System II’ (n572) 8.
1535 Commission, ‘Improved effectiveness’ (n780).
1537 See for instance Stockholm Programme (n606) ¶4.2.2; Council, Document 6975/10 (01.03.2010) pt 20.
interoperability was treated as a matter of urgency.\textsuperscript{1539} In the Communication on stronger and smarter borders, the Commission identified four different models of interoperability, which correspond to a gradation of convergence among the systems:

a. A single search interface to query several information systems simultaneously and to produce combined results on one single screen;

b. Interconnectivity of information systems where data registered in one system will automatically be consulted by another system;

c. Establishment of a shared biometric matching service in support of various information systems; and

d. Common repository of data for different information systems (core module).

With a view to addressing the legal, technical and operational aspects of the different options, including the necessity, technical feasibility and proportionality of available options and their data protection implications, an Expert Group on Information Systems and Interoperability has been set up.\textsuperscript{1540} In the meantime, Member States have already agreed in the Roadmap to enhance information exchange and information management, to implement the first option as a matter of priority, and the remaining options to be discussed in the medium and longer term.\textsuperscript{1541} The undertone for future development is evident and a convergence between criminal law and immigration control systems seems to be in the making. Although the Roadmap refers to all information systems in the AFSJ, related to both immigration and law enforcement, it is explicitly stated that the interlinkages between all different information exchange schemes are highlighted, which ‘will contribute to ensuring the cooperation between the authorities and agencies […] and the interoperability between information systems’.\textsuperscript{1542}

In addition to the aforementioned efforts, interoperability is already embedded in the recent EES and Eurodac proposals. On the one hand, the EES proposal prescribes interoperability between the EES and the VIS in the form of direct communication and consultation.\textsuperscript{1543} Such interconnection is meant to enable border control authorities using the EES to consult the VIS for a series of functions such as: a) to retrieve and import visa-related data to create or update the individual file, including in cases where a visa is annulled, revoked or extended; b) to verify the authenticity and validity of a visa or whether the conditions of entry are met; c) to verify whether a visa-exempt third-country national has been previously registered in the VIS; and d) to verify the identity

\textsuperscript{1539} Council, Document 7371/16 (24.03.2016) pt 5.
\textsuperscript{1541} Council, Document 9368/1/16 (n1519) 5. Also see Council, Document 7711/16 (12.04.2016).
\textsuperscript{1542} ibid 4.
\textsuperscript{1543} For a discussion on interoperability prior to the EES proposal of 2013 see Council, Document 13801/13 (19.09.2013).
of a visa holder through fingerprinting. Furthermore, border control authorities using the
VIS will be able to directly consult EES data when examining visa applications,
whereas visa authorities could update the visa-related data in the EES in the event that a
visa is annulled, revoked or extended.\textsuperscript{1544} On the other hand, the revised Eurodac will be
established in a way that allows for future interoperability with the other databases.\textsuperscript{1545}

Interoperability is a rather complex legal issue with far reaching implications for
individuals, and should not be viewed as a merely technical matter. It significantly
enhances the surveillance powers of the EU by enlarging the number of national
authorities which could have access to the data, and nullifies the limited purposes for
which databases have been set up. In that sense, interoperability ‘disrespects the
importance of separated domains and cuts through their protective walls’.\textsuperscript{1546} Through
the aggregation of information from different systems, a brand powerful system might
emerge.\textsuperscript{1547} Surveillance will be intensified and authorities will be able to draw more
precise conclusions on the private lives of individuals who would not be able to foresee
how the collected information will be used. Individual rights, particularly the right to
information, will be more difficult to exercise. Due to divergent rules regarding several
aspects, such as the retention periods, the inclusion of biometric data or the possibility
of transfers, interoperability may lead to significant revisions in information systems
with a view to aligning the modalities for the sake of efficiency. Interoperability could
thus be seen as the first step to a gradual transition from a compartmentalised system of
independent immigration databases to a single EU information system.

\textbf{6. Conclusion}

This Chapter served to demonstrate that the legal framework on EU immigration
databases is anything but a setting stone. In addition to reforms to the currently
operational systems, a series of ideas are on the EU agenda, which are bound to
progressively extend the reach of the EU in two dimensions. On the one hand, the ever-
growing thirst for as much information as possible is evident; it appears that \textit{all categories}
of third-country nationals, in a generalised manner and without exception,

\textsuperscript{1544} Commission, ‘EES proposal of 2016’ (n982) recital 13 and art 7.
\textsuperscript{1545} Commission, ‘Eurodac proposal of 2016’ (n1003) 5.
\textsuperscript{1546} De Hert and Gutwirth, ‘Interoperability of Police Databases’ (n1536) 7.
\textsuperscript{1547} EDPS, ‘Comments on the Communication of the Commission on Interoperability of European
Databases’ (n1536) 4.
will be required to enroll in different registers. Furthermore, the manufacturing of a cumbersome system of border crossing may render national ‘Trusted Traveller Programmes’ a popular option, resulting in further information collection. On the other hand, through interoperability, the catalogues of third-country nationals will be brought together with unpredictable effects. The EU model for immigration control through information collection and exchange seems to be progressively ‘Americanised’, and privacy protection is superseded in view of security concerns. Since the specifics of these initiatives are yet to be determined, further research will be required in the future.
Conclusion

‘Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts.’

The purpose of this thesis has been to explore the privacy concerns stemming from the establishment and operation of pan-European centralised databases that process personal information collected from different categories of third-country nationals. The topicality of the present research cannot be overstressed. On the one hand, the massive influx into the EU of refugees and migrants, and the structural inability (or unwillingness) of Member States to provide effective protection to individuals in need, has led to a profound re-prioritisation of EU immigration and asylum policy. At the same time, the proliferation of terrorist events and the increased concern about the phenomenon of ‘foreign fighters’ has multiplied the calls for addressing security imperatives also through the convergence of immigration and criminal law. The importance attached to monitoring everyone who is entering or leaving the EU is profound, leading to a strong intensification of border checks not only on third-country nationals but also on EU citizens and the treatment of mobility with paramount suspicion. A key strand of action is the increase in resorting to technological solutions, with the collection and further processing of personal data having become the prime antidote against lack of control of allegedly ‘porous’ borders through which undesirable migrants, terrorists and criminals sneak in. On the other hand, in an era of ‘digital tsunami’, the European Courts have stepped into the surveillance debate and have emerged as the primary guardians of privacy. Judgments such as S and Marper, Digital Rights Ireland and Schrems have made clear that State power is far from unlimited, and have strongly emphasised the need to strike a fair balance between enhancing security whilst safeguarding fundamental rights, particularly privacy.

In this framework, the present thesis has been inspired by, and based upon, these landmark judgments, and has analysed the privacy challenges posed by the setting up

and operation of EU immigration databases. Their legal framework has been viewed through the prism of the right to private life, as enshrined in Articles 7 EUCFR and 8 ECHR. Whereas other legal scholars who have studied this topic have focused on data protection law (either exclusively or in combination with a privacy assessment), this thesis has started from the premise that the right to private life offers more holistic protection to the individuals concerned than the newborn right to the protection of personal data (Article 8 EUCFR). In Chapter 1, I have elaborated on this idea by analysing two main aspects: the centrality of privacy in assessing legal instruments involving the collection, storage and further processing of personal data (such as EU immigration databases); and the constitutive elements of privacy protection in relation to the processing of personal data in a systematic manner, as codified by the jurisprudence of the European Courts. In effect, although prompted by the specific study, this Chapter contributes to knowledge in a more general manner, as its findings are applicable, at least to a certain extent, to other instruments involving the processing of personal data. From the outset, the research hit an obstacle – the lack of a universally agreed definition of privacy. It has been submitted that the understanding of privacy is flexible depending upon jurisdiction and context and, therefore, it may be attached to a multiplicity of notions such as autonomy and dignity. At EU level, the right to private life has been ‘implemented’ in the field of personal data processing through the enactment of numerous general and sectoral data protection instruments, which are caught between a dual rationale; the free flow of data as opposed to the protection of individuals’ privacy. At the constitutional level the framework is more complex due to the elevation of data protection to the status of a fundamental right. In this respect, I have provided two sets of arguments to highlight the centrality of privacy in assessing legal instruments involving the processing of personal data. Firstly, by scrutinising the right to data protection it has been observed that it is not aimed at questioning whether the collection and further processing may take place, but merely provides the ‘rules of the game’, whereas the right to private life, due to its inherent flexibility and robust obligations, provides a more holistic framework for addressing concerns in relation to the processing of personal data. It places an emphasis on the individual and the effect of an instrument in their contemporary life, rather than concentrating on the protection of specific categories of personal data, and can further challenge practices of collecting personal data. The relationship between privacy and data protection is seen as one of mutual reinforcement, whereby the latter is meant to enhance the former rather than function as a replacement, and the right to private life is vital for the right to the protection of personal data which cannot function on its own. Secondly, it has been highlighted that this approach is in line with the case law of the ECtHR and particularly
of the CJEU, which, in a series of judgments, has highlighted both the importance of privacy as the ultimate focal point and the role of data protection *in light of* the right to private life. Having explained the importance of privacy, then I have provided a checklist of criteria to take into consideration when analysing the legal framework of EU immigration databases.

In this framework, Chapters 2-6 I have analysed the legal instruments enacted in relation to the researched information systems, as well as any proposed rules. Since the 1990s, an increasingly dense landscape of large-scale information systems in the field of immigration control has grown out of EU activities questing visibility of migration and travel flows. The EU has resisted the temptation of developing a single, overarching EU-wide system with multiple purposes, and instead has favoured a compartmentalised structure that is ‘more conducive to safeguarding citizens’ right to privacy than any centralised alternative’. The foreign body and its movements have been elevated as the points of reference, and different categories of third-country nationals have been presumed as constituting risky populations, thus necessitating the surveillance of their movement. The timeline of EU immigration databases could be depicted as comprising of three distinct phases amounting to a gradation of surveillance practices. Under the first phase, which largely corresponds to the period between the early 90s until 9/11, the EU legislator seized the opportunity offered by the evolution of technology to equip EU/Schengen governments with two highly sophisticated databases (the SIS and Eurodac) with a two-fold aim – on the one hand, to control the movements of asylum seekers within the EU territory and, on the other hand, to prevent unwanted entry into the EU. The catalysing events of 9/11 have radically transformed the traditional perceptions on performing immigration control. Not only has the VIS been conceptualised in the aftermath of the attacks, but also both the SIS II and Eurodac have been put under the microscope with a view to maximising their functions and exploiting their potential in the fight against terrorism and serious crime. The logic of prevention has been transplanted from its traditional law enforcement context to immigration control and mixed with border control prerogatives on an unprecedented scale. The understanding of surveying the movement of third-country nationals through the construction of centralised databases as normality marks the current third phase of EU immigration databases. Key in this respect is the process of ‘filling gaps’ in information exchange which takes place in a threefold manner: by expanding the requirements of collecting the data to cover any categories of third-country nationals who are unmonitored; by beefing up existing immigration databases through the collection of

---

1549 Commission, ‘Overview of information management’ (n27) 3.
additional categories of personal data, particularly biometric data, which are sensitive information; and ultimately by linking the different ‘data pots’. In effect, the US model is mimicked, at least to a certain extent, even though it has been proven unable to render the US border watertight. Furthermore, throughout the history of immigration databases, it is evident that the rules prescribed in relation to one system, even the problematic ones, may be transplanted to another, in a form of ‘horizontal spillover effect’ of databases. Such examples are the insertion of biometric data in the SIS II and law enforcement access to Eurodac and the EES, which have been clearly triggered by the VIS provisions.

Chapter 2 has focused on the oldest Schengen-wide database (the SIS) and its newest formulation, the SIS II. It has been pointed out that the SIS II interacts with the right to private life in a variety of ways; the system requires the systematic collection, storage and further processing of a series of personal data, including biometric data, which are sensitive information. Furthermore, in terms of the impact to the individual whose data are recorded in the system, the SIS II can, in principle, obstruct their free movement, which may have significant repercussions in maintaining personal relationships or family ties with persons living in the EU. I demonstrated that through its multiple configurations, the SIS II has transformed into a powerful and flexible intelligence tool. Key in this context is the fact that its purpose is vaguely worded, and therefore hinders foreseeability of the implications of the legislation. I observed with concern that the personal scope of the SIS II is steadily expanding by endorsing automaticity in registering alerts and through the mandatory registration of entry bans, and, in the future, return decisions. Due to the lack of clarity regarding the relationship with the Return Directive, recordings of alerts in the SIS II may take place en masse, essentially bypassing the protective clauses of the SIS II Regulation. In effect, the restrictive character of the Return Directive backfires and has collateral repercussions to the SIS II. The inclusion of biometric data is unlawful, not only because the SIS II Regulation explicitly forbids their processing, but also their use for identification purposes is far less reliable, and may have significant repercussions for individuals who are wrongly identified. Furthermore, the insertion of biometrics is indicatory of the transformation of the database to a general intelligence weapon, as it enables ‘fishing’ expeditions, which is evidenced by their use as a search key to uncover links to other alerts in the system. This interlinking of alerts has been identified as another feature of the SIS II that raises significant concerns, as individuals will also be treated on the basis of their possible associations with other persons, which may lead to greater suspicion if they are deemed to be associated with criminals or wanted persons. Finally, the list of authorities designated to access the system, and the lack of control coupled with the
mixed nature of the system, signifies that the specific purposes for which alerts are issued are further eroded.

In Chapter 3, I have examined the case of the VIS, which signaled the beginning of an era whereby a massive number of individuals who are, in principle, unsuspected of any misconduct are placed under surveillance, simply because they pursue legitimate, everyday activities, such as travel. It has been pointed out that the privacy of visa applicants is interfered with not only due to the systematic collection and further processing of personal data, including, but also because on the basis of the collected data it is possible to recreate a rather complete profile of the person concerned, including personal relationships they may hold with EU nationals or other persons lawfully residing in the EU, as well as their personal habits and preferences. Overall, the VIS constitutes a bold move towards the pre-emptive turn of EU immigration control, under the premise that all visa applicants are suspected by default of overstaying or associated with criminal behaviour, irrespective of the legitimacy behind the purpose of their visit to the Schengen territory. Additionally, law enforcement access, which blurs the boundaries between immigration and criminal law, is understood as a further interference with the right to private life. Due to the wide-ranging character of the interference, the importance of data protection in light of the right of privacy, and the administrative nature of the primary objective pursued by the VIS, the proportionality test has been strict. In this respect, I have noted that the collection and further processing of data en masse on all visa applications in a generalised manner and without exceptions is disproportionate to the aims pursued. Furthermore, a series of categories of personal data processed raise concerns, particularly the information on persons or companies issuing an invitation or liable to pay the expenses of the stay to the EU. The collection and storage of two types of biometric data is also problematic, due to the centralised storage which enables abuse and false matches, with potentially significant repercussions to individuals. As for the ‘sweeping’ retention period, this policy choice does not take into account either the different categories of visas or the different outcomes of the visa applications. In relation to the possibility of consulting the VIS data by law enforcement authorities and Europol, I have found that the conditions for access by both the national designated authorities and Europol allow for extensive interpretation, whereas the verification of the conditions of access is conducted by the central access point, the independence of which is doubtful. Any future revision of the already problematic conditions of access is bound to further stigmatise visa applicants. The VIS rules on designating authorities that can have access to VIS data, and on transferring data to third parties, give huge leeway for expanded access by a wide pool of agencies both at national level and worldwide. Besides, the possibility of false
matches has serious repercussions for individuals who may be wrongfully implicated in criminal investigations.

In Chapter 4, the focus has been placed on Eurodac, which is exemplary of the transformation of EU immigration databases over the three phases, as outlined above, with a massive privacy impact on asylum seekers and irregular migrants. With regard to its initial function as a tool meant to support the Dublin mechanism, I have pointed out that the mandatory collection and further processing of a full set of fingerprints in the system interferes with privacy. The proportionality of this interference is doubtful for a series of reasons; the possibility of false matches to persons who are wrongly identified may have significant repercussions for their private life, and disregards the vulnerable positions of asylum seekers. From a functional point of view, the proportionality of Eurodac is questionable, since the Dublin system appears to be unworkable, both for Member States and asylum seekers. The inclusion of irregular residents within the scope *ratione personae* of Eurodac also raises proportionality concerns when performed in a generalised manner, as it happens in certain Member States, unless there are indications that the person in question has applied for international protection. As for the retention period, I noticed that the 10-year storage has not been justified, whereas in cases of persons apprehended irregularly crossing the external border, the retention period goes beyond what is necessary for Dublin-related purposes. The reconfiguration of Eurodac as a weapon deployed in the fight against terrorism and other serious crime constitutes another clear indication of how the boundaries between immigration and police databases are progressively fading. Law enforcement access is a further limitation to privacy which also disregards the vulnerability of applicants for international protection, and denotes that they are considered as a priori suspects of criminality. Although I have observed that the conditions of access mark an improvement compared to the ones stipulated in the VIS Decision, the legislation is nonetheless disproportionate on multiple respects; on the one hand, the necessity of law enforcement access to asylum seekers’ data seems to have been based on the fact that in certain Member States Eurodac data were already stored alongside those of criminals, thus already shared with other Member States under Prüm rules. On the other hand, law enforcement access may lead to increased stigmatisation, particularly if one takes into account the long retention period of fingerprints and the enhanced possibility of false matches in cases when latent fingerprints are compared. Moreover, the recast Eurodac Regulation did not adequately solve certain recurring issues also evident in the VIS framework, such as the designation of competent law enforcement authorities or the nature of the verifying authority. Finally, based on the recent Commission proposal, the system will enable the tracking of all irregular migrants and applicants for international protection through biometrics,
so as to gain intelligence on their preferred routes and, eventually, to prevent and combat irregular migration. In that sense, it will function as a pre-registrar of the SIS II, whereby all third-country nationals without documentation will be placed under surveillance in an indiscriminate manner.

In Chapters 5-6, I have focused on the expected additions to the growing family of EU immigration databases. I have examined the forthcoming EES, which will surpass the VIS in terms of magnitude, and is meant to compensate for the growing tendency to remove third countries from the EU ‘black list’ of countries whose nationals must possess a visa. It has been submitted that the systematic collection, storage and further processing of everyday data interferes with privacy, as it allows drawing certain, rather precise, conclusions about the movements of foreign visitors. However, the added value of setting up the ESS is not fully proven. The operation of the system may significantly disrupt travel flows, thus jeopardising the attainment of its claim to speed up the border crossing process. Furthermore, judging from the US model, which the EES is largely mimicking, the objective of detecting and returning overstayers will only be met to a limited extent. In this framework, and having in mind the many millions of persons who will be subjected to the EES, the lack of proportionality is evident. The requirement of collecting a lesser number of fingerprints has, in turn, been coupled with the addition of a facial image that, in fact, deepens surveillance and signifies no reduction in processing. As for the retention period, the proposed rule is disproportionate in that it equates all travellers irrespective of whether they have lawfully exited or are presumed overstayers. In relation to law enforcement access, the well-established link between immigration control and crime prevention has been once again apparent, to the extent that despite it being an ancillary objective, it has featured prominently in the discussions pre-empting decisions on other key features of the systems. This function has been termed as the ‘vertical spillover effect’ of law enforcement access. Furthermore, I have tried to disprove the points raised in relation to the necessity of law enforcement, showing that few data have been inferred to justify the necessity of this additional functionality. As for the modalities of such access, given that the EES rules are essentially a mixture of VIS and Eurodac provisions, proportionality concerns similar to those already elaborated upon have been raised regarding the strictness of the criteria and the procedure for consulting the data in the course of criminal investigations. However, in the present case, these concerns are exacerbated in light of the huge amount of persons, and the great amount of data, recorded.

Committed to the overarching purpose of this thesis to provide a holistic and up-to-date examination of EU immigration databases, Chapter 6 has outlined other ideas put on the EU table, namely the RTP, the ETIAS, the Residence Permits Repository and the
possibility to interlink databases. With the future introduction of these schemes, surveillance of movement will extend to all categories of third-country nationals in a generalised manner and without exceptions. In effect, in the future there will be no third-country national whose personal data will not be monitored for immigration purposes (and perhaps even for law enforcement purposes as well). Does this mean that EU nationals will be exempt from surveillance practices? As it has been shown in Chapter 5, subjecting EU citizens to checks equivalent to these stipulated for short-stay visitors is not completely off the table. Furthermore, the existing and forthcoming systems will be interconnected, therefore essentially allowing for maximised surveillance through the de facto creation of a gigantic database with grand potential.

Overall, the present study has demonstrated that EU immigration databases constitute a disproportionate form of surveillance of movement of third-country nationals on numerous grounds. Their establishment and operation entails that the lack of EU citizenship seems to ‘entitle’ State authorities to require the provision of a series of personal data, including sensitive ones. Furthermore, the collection and further processing of personal data takes place en masse and increasingly in an indiscriminate manner, and is no longer solely aimed at individuals whose misconduct has attracted the attention of national authorities, but also stems from the pursuit of legitimate activities, such as lodging an asylum application or travelling. Key features are the overreliance on biometric data, despite their inherent limitations and potential for abuse, as well as the focus on centrally registering the collected data rather than pursuing decentralised means of storage. Indeed, it is through centralised storage that databases enable the processing of personal data for a multiplicity of (often divergent) purposes, as no database has a unitary objective any more. Among these purposes, law enforcement has been flagged as a particularly contested issue, not least because the justification of its necessity has often been fragile. However, the stigmatising effect of law enforcement access, particularly since the data are stored for a significant period of time, has been largely disregarded and the modalities of access, albeit fiercely negotiated, allow for significant loopholes. In this framework, it could be even argued that the collection and storage of biometric data in a generalised and indiscriminate manner, which may be further used for various purposes, such as law enforcement, goes to the core of privacy, particularly since it involves very large numbers of individuals who are in principle unsuspected of any misconduct.

Inevitably these conclusions depict the state of play as it is up to 31st July 2016, and research has shown that the legal framework of EU immigration databases is not carved in stone. Since new functionalities are constantly conceived, with a little help from the evolution of technology, and having in mind the moving target that the EU
AFSJ is, further research on the privacy concerns raised by the establishment of new forms of information collection and exchange, particularly interoperability, and the revision of rules on the existing schemes will be necessary.

I would like to conclude this thesis on a positive note. Although it is evident that the EU legislator currently has a highly securitised, far-reaching agenda regarding information exchange, which severely attacks privacy, the role of the European Courts in upholding the right cannot go unnoticed. In an era of omnipotence of personal data processing, both the CJEU and ECtHR have relied on the right to private life to place important limits on State power to carry out pre-emptive surveillance. Therefore, one can only wait to see whether EU immigration databases, which have not yet been litigated in terms of substance, will be challenged before the European Courts in the future. If so, it is hoped that this thesis has provided a comprehensive set of arguments that may be handy in this respect.
References

Legislation

a) EU

i) Conventions - Agreements

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108.


Convention determining the state responsible for examining applications for asylum lodged in one of the Member States of the European Communities [1997] OJ C254/1.


ii) Decisions


Commission Implementing Decision (EU) 2016/281 of 26 February 2016 determining the date from which the Visa Information System (VIS) is to start its operations at external border crossing points [2016] OJ L52/64.


Council Decision 1999/435 of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis [1999] OJ L176/1.


Council Decision of 14 December 2010 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [2010] OJ L333/58.


iii) Framework Decisions


iv) Directives


Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or


v) Regulations


Regulation (EU) 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member States responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) [2013] OJ L180/1.

Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) [2013] OJ L180/31.


Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and

b) US


Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56.


The Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458.

**Commission documents**

**a) Communications**


‘The implementation and development of the common visa policy to spur growth in the EU’ (Communication) COM(2012) 649 final.


‘Functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU’ (Communication) COM(2013) 847 final.


‘Stronger and smarter information systems for borders and security’ (Communication) COM(2016) 205 final.


‘Enhancing security in a world of mobility: Improved information exchange in the fight against terrorism and stronger external borders’ (Communication) COM(2016) 602 final.

b) Proposals


Proposal for a Council Regulation listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement’ COM (2000) 027 final.


‘Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences’ COM(2005) 600 final.

‘Proposal for a Regulation of the European Parliament and the Council concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation (EC) No […] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)’ COM(2008) 825 final.

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

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

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


‘Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)’ COM(2016) 270 final.

‘Proposal for a Regulation of the European Parliament and of the Council on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless persons], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes (Recast version)’ COM(2016) 272 final.

c) Reports


‘The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)’ (Report) COM(2016) 93 final.

d) Studies


‘Preparatory Study to inform an Impact Assessment in relation to the creation of an automated entry/exit system at the external borders of the EU and the introduction of a border crossing scheme for bona fide travellers (‘Registered Traveller Programme’)’ (GHK, 2007).

‘Entry-Exit Feasibility Study’ (UNISYS, 2008).

‘Final Report cost analysis of Entry Exit and Registered Traveller Systems’ (Unisys, 2010).

‘Policy Study on an EU Electronic System for Travel Authorisation’ (PwC, 2011).

‘Fingerprinting recognition for children’ (JRC 2013).

‘Technical Study on Smart Borders’ (PwC 2014).
e) Other Commission documents


____, ‘Staff Working Document – Impact Assessment accompanying Document to the amended proposal for a Regulation of the European Parliament and the Council concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation No […] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version) and to the Proposal of a Council Decision on requesting comparisons with EUROPAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes’ SEC(2009) 936 final.


____, ’“Smart borders”: enhancing mobility and security’ (Press release, 28.02.2013).


_____, ‘Recommendation establishing a common “Return Handbook” to be used by Member States’ competent authorities when carrying our return related tasks’ C2015 6250 final.

**Council documents**


Council, Document 8441/98 (18.05.1998) (Eurodac).


Council, Document 4284/00 (05.05.2000) (Charter).

Council, Document 4102/00 (06.01.2000) (Charter).


Council, Document 12314/00 ADD 1 (15.11.2000) (Eurodac).


Council, Document 5968/02 (05.02.2002) (SIS).

Council, Document 5970/02 (08.02.2002) (SIS).

Council, Document 7309/02 (21.03.2002) (VIS).

Council, Document 9243/02 (27.05.2002) (VIS).


Council, Document 9615/02 (05.06.2002) (VIS).

Council, Document 9620/02 (Presse 175, 13.06.2002) (VIS).

Council, Document 10089/02 (Presse 181, 20.06.2002) (SIS).


Council, Document SN 12463/02 (21/22.06.2002) (SIS).


Council, Document 9182/03 (12.05.2003) (SIS).

Council, Document 9808/03 (26.05.2003) (SIS II).

Council, Document 11638/03 (01.10.2003) (Biometrics).


Council, Document 10125/04 (03.06.2004) (SIS).


Council, Document 6228/05 (Presse 28, 04.03.2005) (VIS).


Council, Document 6811/05 (Presse 42, 14.03.2005) (VIS).
Council, Document 14390/05 (Presse 296, 01/02.12.2005) (VIS).
Council, Document 5596/06 (27.01.2006) (SIS).
Council, Document 5709/1/06 REV 1 ADD 1 (04.04.2006) (SIS).
Council, Document 5709/1/06 REV 1 ADD 7 (05.04.2006) (SIS).
Council, Document 5771/06 (27.01.2006) (EES).
Council, Document 9641/06 (07.06.2006) (VIS).
Council, Document 9083/06 (08.05.2006) (VIS).
Council, Document 9130/06 (08.05.2006) (VIS).
Council, Document 9199/06 (11.05.2006) (VIS).
Council, Document 11062/06 (29.06.2006) (VIS).
Council, Document 11405/06 (03.08.2006) (VIS).
Council, Document 14296/06 (27.10.2006) (SIS).
Council, Document 5049/07 (04.01.2007) (VIS).
Council, Document 5213/07 (11.01.2007) (VIS).
Council, Document 5456/1/07 (20.02.2007) (VIS).
Council, Document 7351/07 (13.03.2007) (VIS).
Council, Document 8198/07 (02.04.2007) (VIS).
Council, Document 8688/07 (16.05.2007) (Eurodac).
Council, Document 9128/07 (02.05.2007) (VIS).
Council, Document 9753/07 (19.06.2007) (VIS).
Council, Document 10002/07 (25.05.2007) (Eurodac).
Council, Document 10267/07 (Presse 125, 25.06.2007) (VIS).
Council, Document 7226/1/09 (18.03.2009) (EES).
Council, Document 6975/10 (01.03.2010) (Interoperability).
Council, Document 7266/12 (07.03.2012) (RTP).
Council, Document 11205/12 (15.06.2012) (SIS).
Council, Document 11861/12 (06.06.2012) (Eurodac).
Council, Document 7476/13 (15.03.2013) (Eurodac).
Council, Document 8018/13 (27.03.2013) (ETIAS).
Council, Document 9863/13 (28.05.2013) (EES).
Council, Document 10720/13 (07.06.2013) (EES).
Council, Document 11143/13 (20.06.2013) (EES).
Council, Document 5386/14 (17.01.2014) (EES).
Council, Document 6040/14 (03.02.2014) (EES).
Council, Document 6626/4/14 (15.05.02014) (EES).
Council, Document 9009/14 (05.05.2014) (*Digital Rights Ireland*).
Council, Document 10720/14 (12.06.2014) (EES).
Council, Document 15922/14 (27.11.2014) (EES).
Council, Document 6747/15 (03.05.2015) (VIS).
Council, Document 8620/15 (07.05.2015) (RTP).
Council, Document 8964/15 (22.05.2015) (RTP).
Council, Document 9778/15 (22.06.2015) (EES).
Council, Document 14382/15 (0.4.05.2016) (EES).
Council, Document 7371/16 (24.03.2016) (Interoperability).
Council, Document 8421/16 (02.05.2016) (EES).
Council, Document 8446/16 (02.05.2016) (EES).
Council, Document 8518/16 (04.05.2016) (EES).
Council, Document 8556/16 (0.4.05.2016) (EES).
Council, Document 8590/16 (03.05.2016) (ETIAS).
Council, Document 8701/16 (12.05.2016) (EES).
Council, Document 9147/16 (20.05.2016) (EES).
Council, Document 9368/1/16 (06.06.2016) (Information exchange).
Council, Document 9387/16 (26.05.2016) (EES).
Council, Document 9578/16 (31.05.2016) (EES).
Parliament documents

Council, Document 10441/16 (28.06.2016) (SIS).

Council, Document 18880/16 (06.07.2016) (EES).


________, ‘Working Document on the Entry/Exit System to register entry and exit data of third country nationals crossing the EU Member States’ external borders; (PE514.706v01-00, 25.6.2013).

________, ‘Working Document on the Entry/Exit System to register entry and exit data of third country nationals crossing the EU Member States’ external borders’ (PE544.477v01-00, 06.01.2015).
Other documents


_____ DOC/02/13 (21/22.06.2002).


eu-LISA, ‘List of designated authorities which have access to data recorded in the Central System of Eurodac pursuant to Article 27(2) of the Regulation (EU) No 603/2013, for the purpose laid down in Article 1(1) of the same Regulation’ (2016).

Initiative of the Kingdom of Spain with a view to adopting the Council Regulation (EC) No …/2002 concerning the introduction of some new functions for the Schengen Information System, in particular in the fight against terrorism [2002] OJ C160/05


Notices from Member States, ‘Declarations concerning Member States’ designated authorities and central access point(s) for access to Visa Information System data for consultation in accordance with Article 3(2) and 3(3) respectively of Council Decision 2008/633/JHA’ [2013] OJ C236/1.

Notices from Member States, ‘List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS)’ [2016] OJ C187/4.

Notices from Member States, ‘List of competent authorities which are authorised to search directly the data contained in the second generation Schengen information system pursuant to Article 31(8) of Regulation (EC) No 1987/2006 of the European Parliament and of the Council and Article 46(8) of Council Decision


**Books, articles, reports, opinions**

-- ‘ECJ upholds VIS access decision’ (2010) 278 *EU Focus* 2010 42.

Ackerman B, *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism* (Yale University Press 2006).


_____, and Marieke de Goede (eds), *Risk and the War on Terror* (Routledge 2008).


final) on the establishment operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final)’ (WP116, 2005).


‘Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)’ (WP237, 2016).


Bayo Belgad J, ‘The Area of Freedom, Security and Justice and the Role of National Courts in the EU Data Protection System’ in Elspeth Guild, Sergio Carrera and
Alejandro Eggenschwiler (eds), The Area of Freedom, Security and Justice Ten Years on - Successes and Future Challenges under the Stockholm Programme (CEPS 2010).


____ and Guild E, ‘Policing at a Distance: Schengen Visa Policies’ in Didier Bigo and Elspeth Guild (eds), *Controlling Frontiers. Free Movement into and within Europe* (Ashgate 2005).


_____*, ‘Extraterritorial Migration Control and Human Rights: Preserving the Responsibility of the EU and its Member States’ in Bernard Ryan and Valsamis Mitsilegas (eds), *Extraterritorial Immigration Control* (Martinus Nijhoff 2010).


_____*, *The Shape of Things to Come* (Statewatch 2008).


Carlyle Breckenridge A, The Right to Privacy (University of Nebraska 1970).


Clayton G, ‘The UK and Extraterritorial Immigration Control’ in Ryan and Mitsilegas (eds), Extraterritorial Immigration Control (Martinus Nijhoff 2010).


Delany H and Carolan E, The Right to Privacy – A Doctrinal and Comparative Analysis (Thomson Round Hall 2008).

Den Boer M (ed), The Implementation of Schengen: First the Widening, Now the Deepening (European Institute of Public Administration 1997).


EDPS, ‘Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by


_____, ‘Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the
establishment of “EURODAC” for the comparison of fingerprints for the effective application of Regulation (EC) No […]/[…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and on the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes’ [2010] OJ C92/1.


_____, ‘Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on migration’ [2012] OJ C34/18.


_____, ‘Opinion of the European Data Protection Supervisor on the proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)’ [2014] OJ C32/25 (executive summary).


_____., ‘Comments of the Electronic Privacy Information Center to the National Protection and Programs Directorate of the Department of Homeland Security – Biometric Data Collection at the Ports of Entry’ (04.06.2013) https://epic.org/apa/comments/EPIC-OBIM-Comments-FINAL.pdf.

Epstein C, ‘Embodying Risk: Using Biometrics to Protect the Borders’ in Louise Amoore and Marieke de Goede (eds), Risk and the War on Terror (Routledge 2008).


Finn R, Wright D and Friedenwald W, ‘Seven Types of Privacy’ in Serge Gutwirth and others (eds), European Data Protection: Coming of Age (Springer 2013).


_____, ‘Fundamental Rights Implications of the Obligation to provide Fingerprints for Eurodac’ (2015).


Fratzke S, 'Not Adding Up: The Fading Promise of Europe’s Dublin System' (Migration Policy Institute 2015).


González Fuster G, The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer 2014).


‘Huber, Marper and Others: Throwing New Light on the Shadows of Suspicion’ (No 8, INEX 2011).

Goold J, ‘Surveillance and the Political Value of Privacy’ (Amsterdam Law Forum 2009).


European Community Law from a Migrant’s Perspective (Kluwer 2001).

‘The Border Abroad – Visas and Border Controls’ in Kees Groenedijk, Elspeth Guild and Paul Milderhoud (eds), In Search of Europe’s Borders (Kluwer 2002).


and Baldaccini A (eds), Terrorism and the Foreigner -: A Decade of Tension around the Rule of Law in Europe (Martinus Nijhoff 2007).

_____ and Bigo D, ‘The Transformation of European Border Controls’ in Bernard Ryan and Valsamis Mitsilegas (eds), Extraterritorial Immigration Control (Martinus Nijhoff 2010).


_____ and others, ‘Enhancing the Common European Asylum System and Alternatives to Dublin’ (PE519.234, Parliament 2015).

Gutwirth S, Privacy and the Information Age (Rowman & Littlefie 2002).

_____ and Niessen J, Immigration and Asylum Law in Europe vol 2 (Kluwer 2001).


_____ and others, Reinventing Data Protection? (Springer 2009).


Hatzis N, ‘Giving Privacy is Due: Private Activities of Public Figures in von Hannover v Germany’ (2005) 16(1) The King’s College Law Journal 143.

Hayes B, ‘From the Schengen Information System to the SIS II and the Visa Information System (VIS): The proposals explained’ (Statewatch 2004).
NeoConOpticon: The EU Security-Industrial Complex (Transnational Institute/Statewatch 2009).


Hernández i Sagrera R, ‘The Impact of Visa Liberalisation in Eastern Partnership Countries, Russia and Turkey on Trans-Border Mobility’ (No 63, CEPS 2014).


Kosta E, Consent in European Data Protection Law (Brill 2013).


____, ‘Article 8 - Protection of Personal Data’ in Steve Peers and others (eds), The EU Charter of Fundamental Rights - A Commentary (Hart 2014).


McCarthy T, The Rights of Publicity and Privacy (1st edn, Clark Boardman Callaghan 1987).


____, EU Criminal Law (Hart 2009).


Parkin J, ‘The difficult road to the Schengen Information System II - The legacy of laboratories and the cost for fundamental rights and the rule of law’ (CEPS 2011).


____ and Nicole Rogers (eds), *EU Immigration and Asylum Law* (Martinus Nijhoff 2006).
and others, *EU Immigration and Asylum Law* vol 3 (Martinus Nijhoff 2012).


Ryan, B and Mitsilegas V (eds), *Extraterritorial Immigration Control* (Martinus Nijhoff 2010).


Schengen JSA, ‘Opinion on the development of the SIS II’ (19.05.2004).


Siemen B, Datenschutz als Europäisches (Duncker & Humblot 2006).


____, Understanding Privacy (Harvard University Press 2008).


____, ‘Fast Capitalism/Slow Terror – Cushy Cosmopolitanism and Its Extraordinary Other’ in Louise Amoore and Marieke de Goede (eds), Risk and the War on Terror (Routledge 2008).


____, ‘Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac’ (CM0712-IV, 2007).

____, ‘Note on the coordination of the relationship between the entry ban and the SIS-alert: an urgent need for legislative measures’ (CM1203, 2012).


____, ‘Note on a proposal for a Directive on combating terrorism’ (CM1603, 2016).
Note on the reforms of the Dublin Regulation, the Eurodac proposal and the proposal for an EU Asylum Agency (CM1609, 2016).


‘Biometric Identification Technologies: Ethical Implications of the Informatization of the Body’ (No 1, Biometric Technology & Ethics 2005).

Vavoula N, ‘The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?’ in Céline Bauloz and others (eds), Seeking Asylum in the European Union:
Selected Protection Issues Raised by the Second Phase of the Common European Asylum System (Brill 2015).


______, Law, Morality, and the Private Domain (Hong Kong University Press 2000).


Case law

a) CJEU


Joined Cases 115/81 and 116/81 Rezguia Adoui v Belgian State and City of Liège (115/81) and Dominique Cornuaille v Belgian State (116/81) [1982] ECR 01665.


Case C-292/97 Karlsson and others [2000] I-02737.


Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU [2008] ECR I-00271.


Case C-553/07 College van burgemeester en wethouders van Rotterdam v M E E Rijkeboer [2009] ECR I-3889.


Joined Cases C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado (24.11.2011).


Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (13.05.2014).

Case C-291/12 Schwarz v Stadt Bochum (17.10.2013).

Joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Ireland (08.04.2014).


Case C-362/14 Maximilian Schrems v Data Protection Commissioner (20.10.2015).

Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15) (pending).

**b) ECtHR**

*Handyside v UK* (1979-80) 1 EHRR.737.

*Tyrer v UK* (1979-80) 2 EHRR 1.

*Klass v Germany* (1979-80) 2 EHRR 214.

*Airey v Ireland* (1979-80) 2 EHRR 305.


*Gaskin v UK* (1990) 12 EHRR 36


Silver v UK (1991) 13 EHRR 582.
Friedl v Austria (1996) 21 EHRR 83.
Loizidou v Turkey (1997) 23 EHRR 513.
Guerra and Others v Italy (1998) 26 EHRR 357.
Amann v Switzerland (2000) 30 EHRR 843.
Rotaru v Romania (2000) 8 BHRC 43.
Özgür Gündem v Turkey (2001) 31 EHRR 49.
Z and others v UK (2002) 34 EHRR 3.
Smith v UK, Appl no 39658/05 (admissibility decision of 04.01.2007).


Mamatkulov and Askarov v Turkey (2005) 41 EHRR 25.

Khelili v Switzerland, Appl no 16188/07 (18.10.2011).


Evans v UK (2008) 46 EHRR 34.


MSS v Belgium and Greece (2011) 53 EHRR 2.


İletmiş v Turkey (2011) 52 EHRR 35.


Nada v Switzerland (2013) 56 EHRR 18.


Szabó and Vissy v Hungary, Appl no 37138/14 (12.01.2016).

c) National courts

Decision BVerfGE 65 1 of the German Constitutional Court of (15.12.1983).

Decision 1 BvR 256/08 of the German Constitutional Court (02.03.2010).

Conseil d’ État, M et Mme Forabosco (no 190384, 09.06.1999).

Decision No 1258 of the Romanian Constitutional Court (08.10.2009).

Decision Pl. ÚS 24/10 of the Czech Constitutional Court (22.03.2011).
Online material


